AD-A056 190 SPERRY UNIVAC ST PAUL MINN DEFENSE SYSTEMS DIV F/G 12/1
COMPLEXITY REDUCTION IN GALOIS LOGIC DESIGN.(U)
DEC 77 J M MARVER N00014-77-C-0192
UNCLASSIFIED PX-12461 NL

| OF |
AD
A056 190

END
DATE
FILMED
8-78
DDC

COMPLEXITY REDUCTION IN GALOIS LOGIC DESIGN

By
J. M. Marver
Sperry Univac
Univac Park
P. O. Box 3525
St. Paul, Minnesota 55165

Report No. PX 12461
Contract No. N00014-77-C-0192
CDRL No. A002

Prepared for:
OFFICE OF NAVAL RESEARCH

DECEMBER 1977

SPERRY UNIVAC
DEFENSE SYSTEMS

12

COMPLEXITY REDUCTION IN GALOIS LOGIC DESIGN

By

J. M. Marver

Sperry Univac
Univac Park
P. O. Box 3525
St. Paul, Minnesota 55165

Report No. PX 12461
Contract No. N00014-77-C-0192
CDRL No. A002

Prepared for:
OFFICE OF NAVAL RESEARCH

DECEMBER 1977

SPERRY UNIVAC
DEFENSE SYSTEMS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

14 **REPORT DOCUMENTATION PAGE**		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER PX-12461	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER 9
4. TITLE (and Subtitle) 6 COMPLEXITY REDUCTION IN GALOIS LOGIC DESIGN.		5. TYPE OF REPORT & PERIOD COVERED FINAL REPORT, FEB–DEC 1977,
		6. ~~PERFORMING ORG. REPORT NUMBER~~
7. AUTHOR(s) 14 J. M./MARVER		8. CONTRACT OR GRANT NUMBER(s) 15 N00014-77-C-0192 new
9. PERFORMING ORGANIZATION NAME AND ADDRESS SPERRY UNIVAC DEFENSE SYSTEMS DIVISION COMPUTER DEVELOPMENT UNIVAC PARK, P.O. BOX 3525 ST. PAUL, MINNESOTA 55165		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS THE OFFICE OF NAVAL RESEARCH DEPARTMENT OF THE NAVY 800 NORTH QUINCY STREET ARLINGTON, VIRGINIA 22217		12. ~~REPORT DATE~~ 11 DEC~~EMBER~~ 1977
		13. ~~NUMBER OF PAGES~~ 12 43p.
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

AS PER CONTRACT

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

GALOIS FIELD
GALOIS MULTIPLIER
PRIMITIVE POLYNOMIAL
SUBFIELD

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

TWO METHODS OF REDUCING THE COMPLEXITY OF THE HARDWARE USED IN GALOIS LOGIC DESIGN ARE PRESENTED: REDUCED TREES OF GALOIS LINEAR MODULES, AND SUBFIELD MULTIPLIERS. THE FIRST METHOD LOWERS THE NUMBER OF MODULES IN A FULL TREE OF GALOIS LINEAR MODULES AND THE SECOND METHOD ENABLES MULTIPLICATION IN A GALOIS FIELD TO BE DONE WITH SUBFIELD MULTIPLIERS.

408 125

ach

TABLE OF CONTENTS

Section		Page
1	INTRODUCTION	1-1
2	GALOIS FIELD DEFINITIONS	2-1
3	METHODS OF COMPLEXITY REDUCTION	3-1
	3.1 Introduction	3-1
	3.2 Sequential Trees	3-1
	3.3 Subfield Multipliers	3-2
4	EXAMPLES	4-1
	4.1 Introduction	4-1
	4.2 Construction of a GF(2^8) Multiplier Using Subfield Multipliers	4-1
	4.3 Construction of a GF(3^4) Multiplier Using Subfield Multipliers	4-11
5	SUMMARY	5-1
6	FUTURE WORK	6-1
	APPENDIX – BASIS PRODUCT MATRICES	A-1
	BIBLIOGRAPHY	

TABLE OF ILLUSTRATIONS

Figure	Title	Page
2-1	External View of Galois Linear Module (GLM)	2-3
2-2	Galois Linear Module Over GF(2^4)	2-4
2-3	A Tree of Galois Linear Modules	2-5
3-1	A Reduced Tree of Galois Linear Modules in GF(2^n)	3-2
4-1	A GF(2^2) Multiplier Over GF(2^1)	4-2
4-2	A Constant t-Multiplier in GF(2^2)	4-4
4-3	A GF(2^4) Multiplier Over GF(2^2)	4-5
4-4	A GF(2^8) Multiplier Over GF(2^4)	4-7
4-5	A Constant g-Multiplier in GF(2^4)	4-8
4-6	A 13-Step GF(2^8) Galois Linear Module (Bit Serial Interface)	4-9
4-7	A GF(3^2) Multiplier Over GF(3)	4-12
4-8	Constant $a^4 = 2$ and a^5 Multipliers	4-14
4-9	A GF(3^4) Multiplier Over GF(3^2)	4-15

LIST OF TABLES

Table	Title	Page
3-1	Cyclotomic Cosets of GF(2^4) Over GF(2^1)	3-4
3-2	Cyclotomic Cosets of GF(2^4) Over GF(2^2)	3-4
3-3	List of Cosets for GF(2^8) (Lowest Exponents Only)	3-9
4-1	A Code for GF(2^2) Over GF(2^1)	4-1
4-2	A Code for GF(2^4) Over GF(2^2) and GF(2^1)	4-3
4-3	Ternary Code for GF(3^2)	4-11
4-4	Ternary Cosets in GF(3^4) with Lowest Exponent in Each Class Named	4-13

SECTION 1
INTRODUCTION

The goal of this report is to describe in detail two solutions to the problem of complexity reduction in the amount of hardware needed to implement a tree of Galois linear modules for the Galois field GF(2^n). The solutions can be broken into two cases: reduction of the number of modules in a tree, and reduction of the complexity of each module. The solution to the first problem is the use of sequential trees, a topic which is discussed in paragraph 3.2. Far more sophisticated is the solution to the second problem. This approach involves the idea of subfield multipliers, and it generalizes to arbitrary Galois fields GF(p^n), p is a prime.

The subject discussed in most of this report is Galois subfield multiplication for arbitrary Galois fields GF(p^n), with a special emphasis on the fields GF(2^n). In the latter fields it has been known for some time that the Galois multiplier designed by J. T. Ellison [1] does the multiplication in the binary field GF(2^1) = {0, 1}. It turns out that for GF(p^n) in general and for GF(2^n) in particular, multiplication can be carried out with arbitrary subfield multipliers. In order to reduce the complexity of the GF(p^n) multiplier, it is necessary to do the multiplication in a sequential mode. The process of subfield multiplication implies a potential for using multi-level logic circuits. If the number of levels is a power of two, subfield multiplication of the elements in GF(2^n) can be done with less hardware and without as much loss of speed as would result if subfield multiplication were done with binary circuits.

Section 2 will be devoted to the known facts that are needed to discuss the reduced trees and subfield multiplication topics in Section 3. Some of this material can be found in previous Sperry Univac reports on Galois logic design, but most can be found only in mathematical textbooks.

In Section 3, two methods of reducing the complexity of a full tree of Galois linear modules are discussed: a reduced tree which lowers the number of modules in a full tree, and a subfield multiplier which reduces the complexity of the individual module. The subfield multiplication can take place for any Galois field GF(p^n), whereas consideration of a reduced tree is relevant only for GF(2^n).

Also in this section a theoretical discussion needed for the generation of larger Galois fields from subfields is given. The remainder of Section 3 is devoted to a detailed exposition of the construction of a GF(2^8) multiplier over GF(2^4) and of a GF(3^4) multiplier over GF(3^2).

Finally, an appendix is added for completeness. In it the basis product matrices used in the construction of GF(p^n) multipliers are discussed.

SECTION 2
GALOIS FIELD DEFINITIONS

Since Galois fields play a central role in this report, a precise definition of a Galois field is given in this section. First, the definition of a mathematical field is necessary.

DEFINITION: Let D be a set of elements a, b, c, ... for which the sum a + b and the product ab of any two elements a and b (distinct or not) of D are defined. Then D is called a field if the following postulates (i) - (x) hold:

(i) Closure. If a and b are in D, then the sum a + b and the product ab are in D;

(ii) Uniqueness. If a = a′ and b = b′ in D, then a + b = a′ + b′ and ab = a′b′;

(iii) Commutative Laws. For all a and b in D, a + b = b + a and ab = ba;

(iv) Associative Laws. For all a, b, and c in D, a + (b + c) = (a + b) + c and a(bc) = (ab)c;

(v) Distributive Law. For all a, b, and c in D, a(b + c) = ab + ac;

(vi) Zero. D contains an element 0 such that a + 0 = a, for all a in D;

(vii) Unity. D contains an element 1 ≠ 0 such that a1 = a for all a ∊ D;

(viii) Additive Inverse. For each a in D, the equation a + x = 0 has a solution x in D;

(ix) Cancellation Law. If c ≠ 0 and ca = cb, then a = b;

(x) Inverse. Every nonzero element a of D has an inverse a^{-1} satisfying the equation a^{-1} a = 1.

By [2,Theorem 6.4], the residue classes of integers modulo any prime number p forms a field of p elements called the *Galois field* GF(p). It can be shown that there is at least one irreducible polynominal of every degree over GF(p) (such a polynomial f is one with no roots in GF(p), i.e., f(y) ≠ 0 for every y in GF(p)) [2, page 155]. In fact, for any positive integer n there is a polynomial f of degree n which generates the Galois field of p^n elements, called $GF(p^n)$ where $GF(p^n) = \{0, t, t^2, \ldots, t^{p^n-1} = 1\}$ for a root t of f. In this case t is called a *primitive element* of $GF(p^n)$ and f is called a *primitive polynomial*. Every element x of $GF(p^n)$ can also be expressed in the form

$$x = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1} \qquad (c_i \text{ in } GF(p)). \qquad (2.1)$$

In this case x is written $(c_0, c_1, \ldots, c_{n-1})$, which is called the p-nary component form of x (if p = 2, it is called the binary form, and if p = 3, it is called the ternary form). The procedure for relating the two representations of x–the power form and the component form–is via the primitive polynomial f. The set of the component forms of all the elements x in $GF(p^n)$ in relation to the power forms of these elements is called *an additive code* for $GF(p^n)$. Such a code has the property that, for $x = (c_0, c_1, \ldots, c_{n-1})$ and $y = (d_0, d_1, \ldots, d_{n-1})$, $x + y = (c_0 \oplus d_0, c_1 \oplus d_1, \ldots, c_{n-1} \oplus d_{n-1})$, where ⊕ denotes addition modulo p.

Multiplication of two elements x and y in $GF(p^n)$ is more easily carried out when x and y are written in their power forms, say $x = t^j$ and $y = t^k$. Then $xy = t^{j+k}$, where j and k are summed modulo $(p^n - 1)$. In the remainder of the paper, for notational convenience, the component form of an arbitrary element of $GF(p^n)$ will be written $c_0 \; c_1 \ldots, c_{n-1}$ instead of $(c_0, c_1, \ldots, c_{n-1})$.

It is well known that every finite field is the Galois field $GF(p^n)$ for some prime p and positive integer n [2, Section 6.5]. It is also true that $GF(p^n)$ minus its 0 element, denoted $GF(p^n) - \{0\}$, is a multiplicative group [2, Section 6.6]. (A group G is a set with a single operation such that the product (sum) of every two elements in G is a third element of G, there is a multiplicative (additive) identity of G, denoted 1 (0), and every element of G has a multiplicative (additive) inverse.) It was pointed out earlier that $t^{p^n-1} = 1$ for a primitive element t of $GF(p^n)$. In fact, $x^{p^n-1} = 1$ for every element $x \neq 0$ in $GF(p^n)$ [2, Theorem 6.18]. The number p^n-1 is called the ***order*** of the group $GF(p^n) - \{0\}$. Since every element x of $GF(p^n) - \{0\}$ is a power of a primitive element t, i.e., $x = t^j$ for some integer j between 1 and p^n-1 ($p^n-1 = 0 \bmod (p^n-1)$), $GF(p^n) - \{0\}$ is a ***cyclic group*** [2, page 157]. In this paper $GF(p^n) - \{0\}$ will often be referred to as the cyclic group of $GF(p^n)$.

Another mathematical structure of interest in this paper is the subfield. A ***subfield*** F of an arbitrary Galois field $GF(p^n)$ is a subset of $GF(p^n)$ which is itself a field under the operations of addition and multiplication in $GF(p^n)$. All subfields of the Galois field $GF(p^n)$ are necessarily $GF(p^m)$ for some integer m dividing n [3, page 447]. It can be seen in equation (2.1) and in the paragraph following (2.1) that every element x in $GF(p^n)$ can be written in its component form $x = c_0 \; c_1 \; \ldots, c_{n-1}$ over $GF(p)$. The set $\{1, t, t^2, \ldots, t^{n-1}\}$ is called a ***basis*** for $GF(p^n)$ over $GF(p)$. More generally, if $GF(p^m)$ is an arbitrary subfield of $GF(p^n)$, then the set $\{1, t, t^2, \ldots, t^{\frac{n}{m}-1}\}$ of n/m elements is a basis for $GF(p^n)$ over $GF(p^m)$. The set $\{1, t, t^2, \ldots, t^{\frac{n}{m}-1}\}$ of $\frac{n}{m}$ elements is a basis for $GF(p^n)$ over $GF(p^m)$. Moreover, by the same method that $GF(p^n)$ can be generated from $GF(p)$ by a primitive polynomial over $GF(p)$ of degree n, $GF(p^n)$ can be generated from $GF(p^m)$ by a primitive polynomial over $GF(p^m)$ of degree $\frac{n}{m}$. Also, every element x in $GF(p^n)$ can be written as

$$x = a_0 \cdot 1 + a_1 \cdot t + \cdots + a_{\left(\frac{n}{m}-1\right)} t^{\frac{n}{m}-1} \tag{2.2}$$

with coefficients $a_0, a_1, \ldots, a_{\left(\frac{n}{m}-1\right)}$ in $GF(p^m)$.

Much of the work on Galois logic design that has been done by Sperry Univac has been concerned with implementation of an arbitrary function/polynomial over the Galois field $GF(2^n)$. The solution to the implementation problem chosen by Sperry Univac is a tree network of Galois linear modules. The Galois linear module, pictured in Figure 2-1 (external view) and in Figure 2-2 (internal view) is basically a $GF(2^n)$ multiplier with a few exclusive – or gates added at the end in order to make a linear function. The tree of linear modules is shown in Figure 2-3. Notice that there are 15 modules in this tree, and that $15 = 2^4 - 1$. For arbitrary n there are $2^n - 1$ Galois linear modules in a full, or universal tree.

Ellison [4] also addressed the problem of doing constant multiplication by a single element of a Galois field. The big advantage of doing constant multiplication is that there is much less circuitry involved than in the full multiplier. The reason that constant multipliers are important in the context of this report is that they are used often in subfield multipliers, as will be seen in Sections 4.2 and 4.3. The constant multipliers described in Ellison in [4] are called Beethoven multipliers and the concept of multiplication by a constant in a Galois field is called Beethoven reduction.

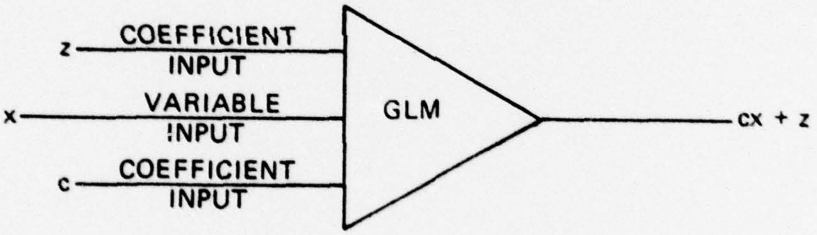

FIGURE 2-1. EXTERNAL VIEW OF GALOIS LINEAR MODULE (GLM)

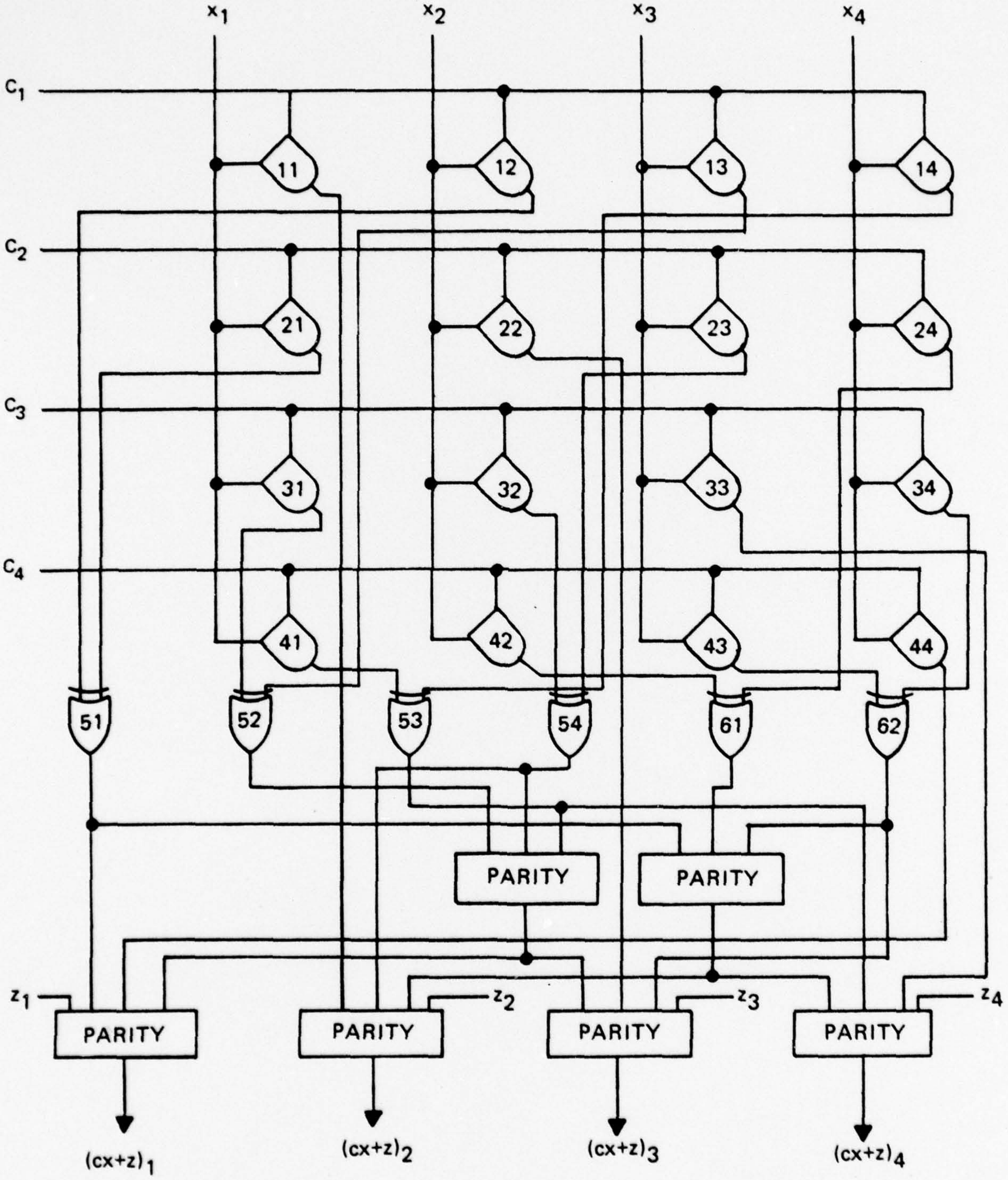

FIGURE 2-2. GALOIS LINEAR MODULE OVER GF(2^4)

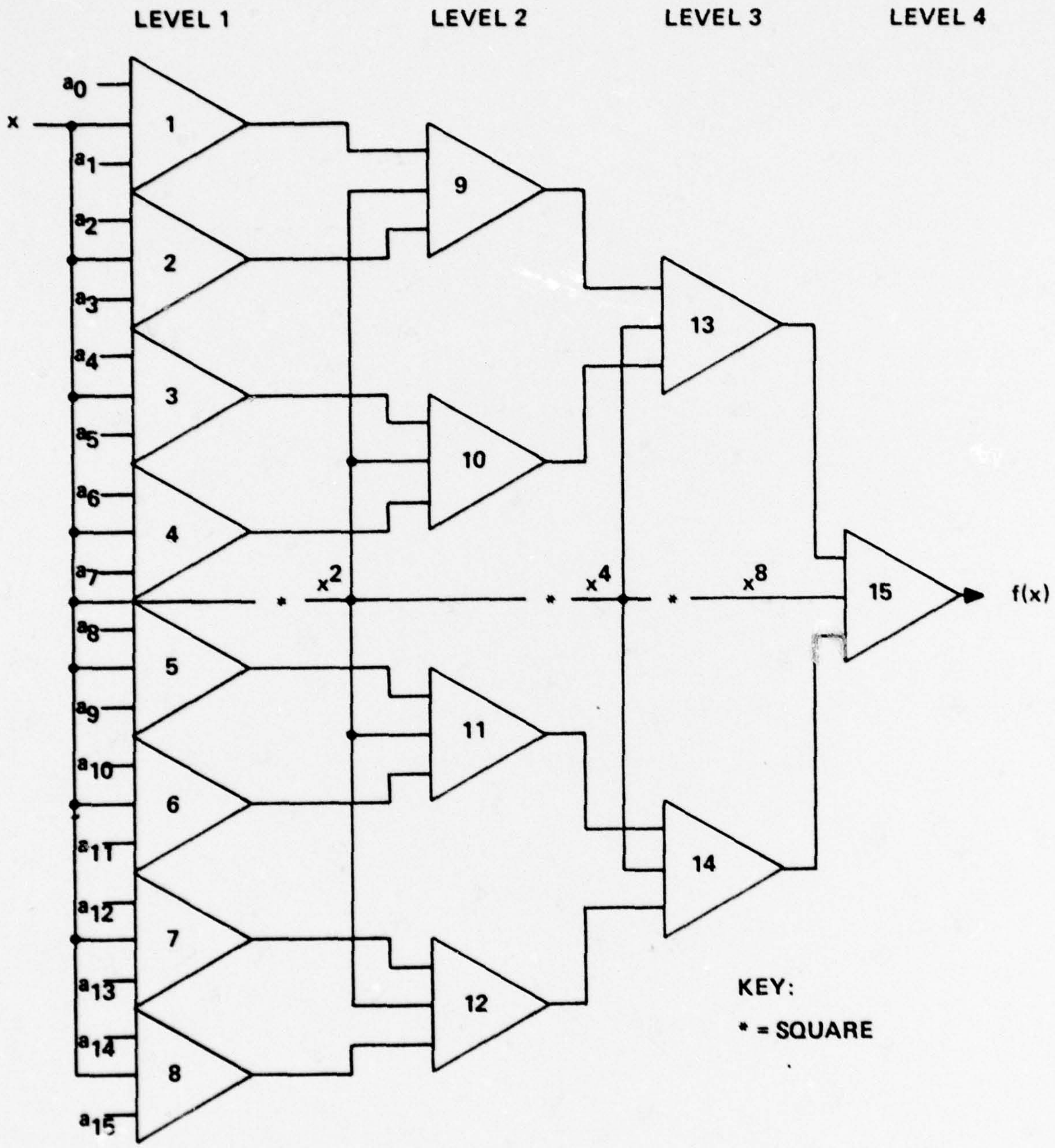

FIGURE 2-3. A TREE OF GALOIS LINEAR MODULES

SECTION 3
METHODS OF COMPLEXITY REDUCTION

3.1 INTRODUCTION

The original thrust of Galois logic design was a *universal one. In fact, for the most part, the research done* to date has been directed toward designing circuits capable of doing arbitrary functions in a Galois field. Thus, the complexity of Galois circuits has been greater than if the circuits were devised for a specific function. In order to maintain the generality with a more reasonable amount of hardware, methods of reducing the complexity of the Galois circuits were studied. Two different approaches were investigated: a reduction in the number of modules in a tree, and a reduction in the size of a module by doing subfield multiplication. In this section these two methods will be discussed; Section 3.2 deals with sequential trees and Section 3.3 considers subfield multipliers.

3.2 SEQUENTIAL TREES

For a full tree of GF(2^n) Galois linear modules there are (2^n - 1) modules, as it was pointed out in Section 2. For large n, (2^n - 1) can be prohibitively large and so it is of interest to reduce the number of modules in a full tree without losing computing capability. It turns out that if n is an even integer, say n = 2k, then

$$2^n - 1 = 2^{2k} - 1 = (2^k)^2 - 1^2 = (2^k - 1)(2^k + 1). \qquad (3.1)$$

This factorization of the number of modules in a GF(2^n) tree into two numbers, one of which is the number of modules in a full GF(2^k) tree, suggests that sequential operation of a GF(2^k) tree with (2^k + 1) passes will simulate a GF(2^n) tree. Figure 3-1 is a reduced tree of ($2^{n/2}$ - 1) = 2^k - 1 Galois linear modules. The first $2^{n/2}$ passes are made with the coefficients of the polynomial and the outputs f_1, are stored in a storage register. The final pass is made with these outputs used as the coefficients, at which time the variable inputs of each module are altered in order to allow for the change in the levels of the original tree that the reduced tree simulates in its last pass.

For a given n there may be many factorizations of $(2^n - 1)$. For example, if n is even there are always other factorizations of $(2^n - 1)$ other than $\left(2^{n/2} - 1\right) \left(2^{n/2} + 1\right)$ [2, page 474]. In fact $(2^n - 1)$ has 3 as a factor since $2^{n/2} - 1$ and $2^{n/2} + 1$ are two consecutive odd numbers encompassing $2^{n/2}$, which clearly does not have 3 as a factor. Therefore, either $2^{n/2} - 1$ or $2^{n/2} + 1$ has a factor of 3. Thus, for even n, a full tree of $(2^n - 1)$ Galois linear modules can be replaced either by a tree of $2^{n/2} - 1$ modules or by a tree of $(2^2 - 1) = 3$ modules. It is also important to observe that for odd n, $2^n - 1$ may be prime: for example, if $n = 3$ or 5, $2^n - 1$ is prime.

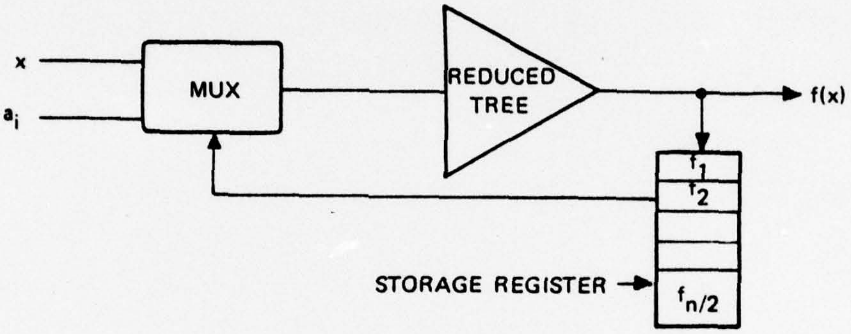

FIGURE 3-1. A REDUCED TREE OF GALOIS LINEAR MODULES IN GF(2^n)

Note that in the description given above only the size of the tree is altered. The size of the individual modules remains the same. The amount of hardware involved in the individual modules can be reduced also, which is the subject of the next paragraph. The advantages of the two concepts of hardware reduction, when combined, should be the subject of a future study.

3.3 SUBFIELD MULTIPLIERS

The theoretical background needed to develop the idea of Galois subfield multiplication begins with the fact that every Galois field can be generated from any one of its subfields by a primitive polynomial over that subfield by the method described in Section 2. If GF(p^n) is the larger field, and if GF(p^m) is a subfield of GF(p^n), then m divides n, and there exists at least one primitive polynomial of degree n/m over GF(p^m) which generates GF(p^n). [2, Section 6.6]. For each primitive polynomial there are several bases which can be used to develop the code for the larger field. The process which will be discussed below for doing subfield multiplication suggests using for a basis the (n/m) elements of GF(2^n), $1, \gamma, \gamma^2, \ldots, \gamma^{(n/m)-1}$ (here γ is a root of the selected primitive polynomial. This basis allows for an easier determination of the code representation of the larger field written with the elements of GF(2^n) as coefficients (see equation (2.2)). In the remainder of this paragraph the theoretical aspects of subfield multiplication are discussed. Let n be a positive integer and consider the Galois field GF(p^n). Let γ be a primitive element of GF(p^n). The minimum polynomial of γ^k for any positive integer k is the polynomial of lowest degree over GF(p) for which γ^k is a root. All elements of GF(p^n) which have the same minimum polynomial as γ^k are called *conjugate elements* of γ^k [5]. The totality of such elements forms a so-called *cyclotomic coset.* Since every element of the coset is a root of the same minimum polynomial, the size of the coset is the same as the degree of the corresponding minimum polynomial. In view of the fact that the minimum polynomial of each coset divides the polynomial $x^{p^n} - x$ [2, Theorem 6.23], and that the minimum polynomials are irreducible [2, Theorem 6.15], the minimum polynomial of each coset has degree less than or equal to n [2, Theorem 6.24]. Hence, the number of elements in each coset of GF(p^n) is less than or equal to n. It is well-known that if γ is an element of GF(p^n) with minimum polynomial f(x) of degree k, then $\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{k-1}}$ are all the roots of f(x) [2, Theorem 6.25]. Hence, the coset of γ is precisely $\{\gamma, \gamma^p, \ldots, \gamma^{p^{k-1}}\}$. More generally, if the base field is an arbitrary subfield GF(p^m) of GF(p^n) instead of GF(p), the concepts of minimum polynomial, conjugation, and cyclotomic cosets over GF(p^n) carry over from GF(p). In particular, the following proposition gives a description of these generalized cyclotomic cosets.

PROPOSITION 3.1: Let γ be a primitive element of GF(p^n) and let j be any positive integer less than n. If m is a positive integer dividing n, say n = md, *then the set of conjugates of* γ^j *(including* γ^j*) with respect to* GF(p^m) is precisely the set of elements $\{(\gamma^j)^{p^{tm}} \mid t = 0, 1, \ldots, d-1\}$.

Proof: Recall that two elements are conjugates if they satisfy the same irreducible polynomial. Thus, if $f(x) = x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ is an irreducible polynomial of degree d over GF(2^m) with root γ^j, then

$$
\begin{aligned}
f\left((\gamma^j)^{p^{tm}}\right) &= \left((\gamma^j)^{p^{tm}}\right)^d + a_{d-1}\left((\gamma^j)^{p^{tm}}\right)^{d-1} + \cdots + a_1 (\gamma^j)^{p^{tm}} + a_0 \\
&= (\gamma^{jd})^{p^{tm}} + a_{d-1}^{p^{tm}} \left(\gamma^{j(d-1)}\right)^{p^{tm}} + \cdots + a_1^{p^{tm}} (\gamma^j)^{p^{tm}} + a_0^{p^{tm}} \\
&= \left((\gamma^j)^d + a_{d-1} (\gamma^j)^{(d-1)} + \cdots + a_1 \gamma^j + a_0\right)^{p^{tm}} \\
&= 0
\end{aligned}
$$

Note that $(a_i)^{p^{tm}} = a_i$, since a_i is an element of GF(p^n) for every i = 0, 1, . . ., d-1 and for every t = 0, 1, . . ., d-1.

It should be pointed out that there may be fewer than $\frac{n}{m} = d$ distinct conjugates of γ^j, a situation which can arise only if j is a divisor of $p^n - 1$.

Recall from Section 2 that every Galois field can be generated from any of its subfields by a primitive polynomial over the subfield. The primitive polynomials are among the minimum polynomials of elements of the subfield (all minimum polynomials are irreducible, but are not necessarily primitive). It is of interest to know which minimum polynomials are primitive to see the various paths with which to form a larger field from a subfield. It will be shown below that minimum polynomials which are primitive can be distinguished from nonprimitive polynomials by looking at the corresponding cyclotomic cosets. First, though, two examples of a breakdown of $GF(2^4)$ into cyclotomic cosets are $GF(2^1)$ and $GF(2^2)$ are given in Tables 3-1 and 3-2. Also listed are the corresponding minimum polynomials. In Table 3-2, the element t of $GF(2^2)$ is a root of $x^2 + x + 1$.

TABLE 3-1. CYCLOTOMIC COSETS OF $GF(2^4)$ OVER $GF(2^1)$ [2, PAGE 476]

COSETS	MINIMUM POLYNOMIAL	PRIMITIVE
1. $\{g, g^2, g^4, g^8\}$	$x^4 + x^3 + 1$	YES
2. $\{g^3, g^6, g^{12}, g^9\}$	$x^4 + x^3 + x^2 + x + 1$	NO
3. $\{g^5, g^{10}\}$	$x^2 + x + 1$	NO
4. $\{g^7, g^{14}, g^{13}, g^{11}\}$	$x^4 + x + 1$	YES
5. $\{g^{15} = g^0 = 1\}$	$x + 1$	NO

TABLE 3-2. CYCLOTOMIC COSETS OF $GF(2^4)$ OVER $GF(2^2)$

COSETS	MINIMUM POLYNOMIAL	PRIMITIVE
1. $\{g, g^4\}$	$x^2 + t x + t$	YES
2. $\{g^2, g^8\}$	$x^2 + t^2 x + t^2$	YES
3. $\{g^3, g^{12}\}$	$x^2 + tx + 1$	NO
4. $\{g^6, g^9\}$	$x^2 + t^2 x + 1$	NO
5. $\{g^5\}$	$x + t$	NO
6. $\{g^{10}\}$	$x + t^2$	NO
7. $\{g^7, g^{13}\}$	$x^2 + x + t$	YES
8. $\{g^{11}, g^{14}\}$	$x^2 + x + t^2$	YES
9. $\{g^{15} = 1\}$	$x + 1$	NO

A necessary condition that a coset correspond to a primitive polynomial, i.e., that the minimum polynomial of the coset have primitive elements for its roots, is that the coset contain n distinct elements. However, this condition is not sufficient, as can be seen in Table 3-1 by the coset $\{g^3, g^6, g^{12}, g^9\}$. The reason that this coset does not consist of primitive elements is that the exponents 3, 6, 12, and 9 have the common factor of 3 with the order, $15 = 2^4 - 1$, of the cyclic group $GF(2^4) - \{0\}$. Since cosets with fewer than n elements correspond to cosets in subfields of $GF(2^n)$, the minimum polynomials corresponding to them cannot be primitive. Thus, in order to determine the primitive polynomials of $GF(2^n)$ over $GF(2^1)$, one first computes the number of n-element cosets of $GF(2^n)$, and then discards the remaining cosets whose elements have exponents having a common factor (larger than 1) with $(2^n - 1)$, the order of the cyclic group $GF(2^n) - \{0\}$ of $GF(2^n)$. In Proposition 3-3 below there is a procedure given for counting the number of n-element cosets. However, Lemma 3-2, which involves the concept of greatest common divisor, is needed first.

A few facts concerning the greatest common divisor are now in order. Let $n = p_1{}^{k} \cdot p_2{}^{k_2} \ldots p_t{}^{k_t}$, the p_i's distinct primes. Then $n/p_1, n/p_2, \ldots, n/p_t$ are all divisors of n, in fact, maximal proper divisors of n, and so $GF(p^{n/p_i})$ is a maximal subfield of $GF(p^n)$ for every i. In other words, there are no proper nonzero subfields (i.e., not $GF(p^n)$) of $GF(p^n)$ containing $GF(p^{n/p_i})$. The largest number which is a divisor of two numbers a and b is called the greatest common divisor of a and b, and is written gcd (a, b); for example, gcd (6, 15) = gcd $(2 \cdot 3, 3 \cdot 5) = 3$.

Lemma 3-2 helps to get an exact count of the number of cosets displayed in Proposition 3-3.

LEMMA 3-2: Let n be a positive integer and suppose that $n = p_1{}^{k_1} \cdot P_2{}^{k_2} \cdots p_t{}^{k_t}$, each p_i a distinct prime, and each k_i a positive integer. Then the greatest common divisor of $n/p_1, n/p_2, \cdots, n/p_t$ (g cd $(n/p_1, n/p_2, \ldots, n/p_t)$) is $p_1{}^{k_1-1} \cdot p_2{}^{k_2-1} \cdots p_t{}^{k_t-1}$.

Proof: Let $y = p_1{}^{k_1-1} \cdot p_2{}^{k_2-1} \cdots p_t{}^{k_t-1}$. Now note that $\frac{n}{p_i} = p_1{}^{k_1} \cdot p_2{}^{k_2} \cdots p_i{}^{k_i-1} \cdots p_t{}^{k_t}$

for every $i = 1, 2, \ldots, t$. Therefore, y divides n/p_i for every $i = 1, 2, \ldots, t$, and so y divides gcd $(n/p_1, n/p_2, \ldots, n/p_t)$. Suppose d is an integer such that yd = gcd $(n/p_1, n/p_2, \ldots, n/p_t)$. If d is greater than 1, then $d = p_i{}^{j_1} \cdot p_2{}^{j_2} \cdots p_t{}^{j_t}$ where at least one of the j_i's is greater than 0, say j_1. Then

$$yd = \left(p_1{}^{k_1-1} \cdot p_2{}^{k_2-1} \cdots p_t{}^{k_t-1}\right) \cdot \left(p_1{}^{j_1} \cdot p_2{}^{j_2} \cdots p_t{}^{j_t}\right) = p_1{}^{k_1-1} \cdot \tag{3.2}$$

$$p_1{}^{j_1} \cdot (\text{extraneous}) = p_1{}^{(k_1-1)+j_1} \cdot (\text{extraneous}).$$

(The extraneous part is not important to this argument.) Since yd is the greatest common divisor of $n/p_1, \ldots n/p_t$, yd divides $n/p_1 = p_1{}^{k_1-1} \cdot p_2{}^{k_2} \cdots p_t{}^{k_t}$ and so, from (3.2),

$j_1 = 0$, a contradiction to the original assumption that j_1 is greater than 0. Thus, $j_i = 0$ for all $i = 1, 2, \ldots, t$ and so $d = 1$ and finally $y = \gcd(n/p_1, n/p_2, \ldots, n/p_t)$.

PROPOSITION 3-3: Let n be a positive integer and p be prime, and suppose that $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_t^{k_t}$, the p_i's distinct primes. Then the number T of n-element cyclotomic cosets of $GF(p^n)$ with respect to $GF(p)$ is

$$T = \frac{1}{n}\left\{p^n - \sum_{i=1}^{t} p^{n/p_i} + \sum_{k \geqslant j} \sum_{j=1}^{\binom{t}{2}} p^{\gcd(n/p_j,\, n/p_k)} - \sum_{a,\,b,\,c,\,d} p^{\gcd(\gcd(n/p_a,\, n/p_b),\, \gcd(n/p_c,\, n/p_d))} + \cdots \pm p^{p_1^{k_1-1} \cdot p_2^{k_2-1} \cdots p_t^{k_t-1}}\right\}$$

Proof: The proof consists of counting the number of elements in $GF(p^n)$ which lie in cyclotomic cosets of length n, and then dividing by n.

The first step is to subtract from p^n, the total number of elements in $GF(p^n)$, the totality of elements of $GF(p^n)$ which lie in maximal subfields of $GF(p^n)$. The number of such elements is $\sum_{i=1}^{t} p^{n/p_i} = p^{n/p_1} + p^{n/p_2} + \ldots + p^{n/p_t}$, i.e., all the elements in the maximal subfields of $GF(p^n)$. However, unless $t = 1$ (i.e., n is the power of a single prime number) there are nontrivial intersections among the maximal subfields and so there are some elements which have been subtracted more than once. Since the intersection of the two maximal subfields $GF(p^{n/p_j})$ and $GF(p^{n/p_k})$ has gcd $(p^{n/p_j}, p^{n/p_k})$ elements for $j, k = 1, 2, \ldots, t$, the number of elements in all of these intersections is

$$\sum_{k \geqslant j} \sum_{j=1}^{\binom{t}{2}} p^{\gcd(n/p_j,\, n/p_k)},$$

and this sum must be added to the total. Once again, there may be a nontrivial intersection of the fields $GF(p^{\gcd(n/p_a,\, n/p_b)})$ and $GF(p^{\gcd(n/p_c,\, n/p_d)})$ for some a, b, c, d. Hence, the sum

$$\sum_a \sum_b \sum_c \sum_d p^{\gcd\left(\gcd(n/p_a,\, n/p_b),\, \gcd(n/p_c,\, n/p_d)\right)}$$

must be subtracted from the previous total. This process continues until all the pairwise intersections are the same, at which point the number of elements in this subfield is added or subtracted. The final sum is the total of all the elements which do not lie in any proper subfield of $GF(p^n)$, and therefore which do not lie in any coset of length less than n. This total is $p_1^{k_1-1} \cdot p_2^{k_2-1} \cdots p_t^{k_t-1}$, since it is equal to $\gcd(n/p_1, n/p_2, \ldots, n/p_t)$ (see Lemma 3-2). Dividing by n now gives the number of n-element cosets.

COROLLARY 3-4: Let n be a positive integer and p a prime. If m is a divisor of n, then the number of n/m-element cyclotomic cosets in $GF(2^n)$ over $GF(2^m)$ is mT.

Proof: Since one needs a primitive polynomial of degree n/m over $GF(2^m)$ to generate $GF(2^n)$, the maximum length of a coset in $GF(2^n)$ over $GF(2^m)$ is n/m.

There are T n-element cosets in $GF(2^n)$ and so there are no fewer than (m T) n/m-element cosets in $GF(2^n)$ over $GF(2^m)$ (since there are a total of nT elements in these cosets, and $nT = (n/m)\,(mT)$).

In fact, there can be no other cosets of length n/m, since they would have been part of an n-length coset over $GF(2^n)$, originally, by the definition of a cyclotomic coset.

The following three examples will help illustrate the preceding two results.

EXAMPLE 3-5: Let p = 2 and $n = 12 = 2^2 \cdot 3$. Then $p_1 = 2$ and $p_2 = 3$, and so $n/p_1 = 12/2 = 6$ and $n/p_2 = 12/3 = 4$. Thus, the maximal subfields of $GF(2^{12})$ are $GF(2^6)$ and $GF(2^4)$, and the intersection of these two subfields is the subfield $GF(2^{\gcd(6,4)}) = GF(2^2)$. Hence, the number of elements in $GF(2^{12})$ of order 2^{12}-1 is

$$2^{12} - \{2^6 + 2^4\} + 2^2 = 4096 - \{64 + 16\} + 4 = 4096 - 76 = 4020$$

and so the number of 12 element cosets in $GF(2^{12})$ is 4020/12 = 335.

EXAMPLE 3-6: Let p = 3, and $n = 15 = 3 \cdot 5$. Then $p_1 = 3$ and $p_2 = 5$, and so $n/p_1 = 15/3 = 5$ and $n/p_2 = 15/5 = 3$. Thus, the maximal subfields of $GF(3^{15})$ are $GF(3^5)$ and $GF(3^3)$. Since $\gcd(3, 5) = 1 = 3^0 \cdot 5^0$, the intersection of these two subfields is $GF(3^1)$, and so there are

$$3^{15} - \{3^5 + 3^3\} + 3^1$$

elements of order $(3^{15} - 1)$ in $GF(3^{15})$. Thus, there are

$$\frac{3^{15} - \{3^5 + 3^3\} + 3^1}{15} = \frac{14{,}348{,}907 - 270 + 3}{15} = \frac{14{,}348{,}640}{15} = 956{,}576$$

15-element cosets in $GF(3^{15})$.

EXAMPLE 3-7: Let $p = 2$ and $n = 360 = 2^3 \cdot 3^2 \cdot 5$. Then $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$. Hence, $n/p_1 = 360/2 = 180$, $n/p_2 = 360/3 = 120$, and $n/p_3 = 360/5 = 72$. Thus, the maximal subfields of $GF(2^{360})$ are $GF(2^{180})$, $GF(2^{120})$, and $GF(2^{72})$. Next, gcd(180, 120) = 60, gcd(180, 72) = 36, and gcd(120, 72) = 24. Finally, gcd(60, 36) = gcd(60, 24) = gcd(36, 24) = 12. Note also that $p_1^{k_1-1} \cdot p_2^{k_2-1} \cdot p_3^{k_3-1} = 2^2 \cdot 3^1 \cdot 5^0 = 4 \cdot 3 \cdot 1 = 12$. Thus, the number of 360-element cosets in $GF(2^{360})$ is

$$\frac{1}{360}\left\{2^{360} - \left[2^{180} + 2^{120} + 2^{72}\right] + \left[2^{60} + 2^{36} + 2^{24}\right] - 2^{12}\right\}.$$

Since the cosets of length n in $GF(p^n)$ correspond to irreducible polynomials (recall that all minimal polynomials are irreduciole), Proposition 3-3 gives the number of irreducible polynomials over the base field GF(p). To determine which of these polynomials are primitive, it is sufficient to observe if the exponent of any element of a coset has a factor (other than 1) in common with the order of the field $p^n - 1$. If there is such a factor, the corresponding minimum polynomial is not primitive (because the elements of the coset cannot be primitive elements of the field); otherwise it is primitive. The next example illustrates this principle.

EXAMPLE 3-8: Let $p = 2$ and $n = 8 = 2^3$. Since 8 is the power of a single prime it is necessary to subtract only the single maximal subfield $GF(2^4)$ of $GF(2^8)$, i.e., there are

$$\frac{1}{8}\left\{2^8 - 2^4\right\} = \frac{1}{8}\left\{256 - 16\right\} = \frac{1}{8}(240) = 30$$

cosets in $GF(2^8)$ with 8 elements (see [2, page 476] – note that there are 16 irreducible polynomials of degree 8 listed there. Fourteen of those have different reciprocals and two are self-reciprocal. Thus, there are 14 x 2 + 2 = 30 distinct irreducible polynomials listed there). To determine the number of primitive polynomials, the order of $GF(2^8) - \{0\} = 2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$ is needed. In Table 3-3, the lowest exponent of each cyclotomic coset is listed and whether the corresponding minimum polynomial is primitive. (Note that all the cosets which are not associated with a primitive polynomial have lowest exponent having a common factor with 255.)

Note that if γ^1 represents a primitive element from the first coset, then γ^{17}, γ^{51}, γ^{85}, γ^{119}, and $\gamma^{255} = \gamma^0 = 1$ represent the different cosets of $GF(2^4)$ (all the elements except 0 are accounted for).

It is often necessary to generate the Galois field $GF(p^{2n})$ from $GF(p^n)$ with a primitive polynomial of degree 2 over $GF(p^n)$. It is possible to choose a primitive element in $GF(p^{2n})$ and its conjugate with respect to $GF(p^n)$ (see Proposition 3-1) and calculate a primitive polynomial of degree two. For designing the Galois multiplier for $GF(p^{2n})$ by doing the actual multiplication over $GF(p^n)$, it is necessary to know how to write the primitive element and its conjugate with coefficients in $GF(p^n)$. The next proposition tells exactly how to do that.

TABLE 3-3. LIST OF COSETS FOR GF(2^8) (LOWEST EXPONENTS ONLY)

	LOWEST			LOWEST			LOWEST	
COSET	EXPONENT	PRIMITIVE	COSET	EXPONENT	PRIMITIVE	COSET	EXPONENT	PRIMITIVE
1.	1	YES	13.	25	NO	25.	59	YES
2.	3	NO	14.	27	NO	26.	61	YES
3.	5	NO	15.	29	YES	27.	63	NO
4.	7	YES	16.	31	YES	28.	85	(2 ELEMENTS)
5.	9	NO	17.	37	YES	29.	87	NO
6.	11	YES	18.	39	NO	30.	91	YES
7.	13	YES	19.	43	YES	31.	95	NO
8.	15	NO	20.	45	NO	32.	111	NO
9.	17	(4 ELEMENTS)	21.	47	YES	33.	119	(4 ELEMENTS)
10.	19	YES	22.	51	(4 ELEMENTS)	34.	127	YES
11.	21	NO	23.	53	YES	35.	255	(1 ELEMENT)
12.	23	YES	24.	55	NO			

PROPOSITION 3-9: Let p be a prime number and let n be a positive integer. Suppose that α is a primitive element of GF(p^n) and that $f(x) = x^2 + \alpha^i x + \alpha^k$ is a primitive polynomial over GF(p^n) generating GF(p^{2n}). If γ is a root of f, and if n is a positive integer, then the conjugate element $(\gamma^m)^{p^n}$ of $\gamma^m = s + t\cdot\gamma$ with respect to GF(p^n) is

$$\gamma^{m\cdot p^n} = [(p-1)t\cdot\alpha^i + s]\cdot 1_{2n} + (p-1)t\cdot\gamma \tag{3.3}$$

for s and t in GF(p^n). In particular if γ^m is an element of GF(p^n), i.e., if $t = 0$, then γ^m is self-conjugate.

Proof: Since γ^m and $(\gamma^m)^{p^n}$ are conjugates with respect to GF(p^n) by Proposition 3-1, then they are the two roots of a quadratic polynomial over GF(p^n). In fact, they satisfy the polynomial

$$(x-\gamma^m)(x-\gamma^{mp^n}) = x^2 - (\gamma^m + \gamma^{mp^n}) + \gamma^m\cdot\gamma^{mp^n}$$

and so the coefficients $\gamma^m + \gamma^{mp^n}$ and $\gamma^m\cdot\gamma^{mp^n}$ must lie in GF(p^n). Suppose $\gamma^{mp^n} = a + b\cdot\gamma$. Then

$$\gamma^m + \gamma^{mp^n} = (s + t\cdot\gamma) + (a + b\cdot\gamma) = (s+a) + (t+b)\gamma \tag{3.4}$$

and

$$\gamma^m \cdot \gamma^{mp^n} = (s + t \cdot \gamma)(a + b \cdot \gamma) = sa + (ta + sb)\gamma + tb\gamma^2 \tag{3.5}$$

$$= sa + (ta + sb)\gamma + tb[-(\alpha^j\gamma + \alpha^k)] = sa + (ta + sb)\gamma + (p - 1)[\alpha^j\gamma + \alpha^k]tb$$

$$= \left(sa + (p - 1)\alpha^k tb\right) 1_{2n} + [ta + sb + (p - 1)\alpha^j tb]\gamma .$$

Since $\gamma^m + \gamma^{mp^n}$ and $\gamma^m \cdot \gamma^{mp^n}$ are in $GF(p^n)$ and since elements of $GF(p^{2n})$ which lie in $GF(p^n)$ are written $h \cdot 1_{2n} + 0_n \cdot \gamma$ for some h in $GF(p^n)$,

$$t + b = 0 \qquad \text{from (3.4) and } ta + sb + (p - 1)\alpha^j tb = 0 \text{ from (3.5).}$$

Thus, $b = -t = (p - 1)t$ and together with the fact that $(p - 1)^2 = 1 \pmod p$ (since $p - 1 = -1 \pmod p$), $0 = ta + s(p - 1)t + (p-1)\alpha^j t(p - 1)t = t\left(a + (p - 1)s + \alpha^j t\right)$. Finally, $t = 0$ or $a + (p - 1)s + \alpha^j t = 0$.

If $t \neq 0$, then $a + (p - 1)s - \alpha^j t = 0$, and so $a = -(p - 1)s - \alpha^j t = s + (p - 1)\alpha^j t$. Thus, $\gamma^{mp^n} = [s + (p - 1)\alpha^j t] + (p - 1)t \cdot \gamma$, which agrees with (3.3).

If $t = 0$, then $b = -t = 0$, and so $\gamma^{mp^n} = a \cdot 1 + 0 \cdot \gamma = a \cdot 1$. Also, since $\gamma^{mp^n} = (\gamma^m)^{p^n} = (s \cdot 1)^{p^n} = s^{p^n} \cdot 1 = s \cdot 1$, $a = s$ and γ^m is self-conjugate.

The next example, which illustrates the preceding proposition, will be discussed in more detail in the next section. That discussion occurs in the exposition of the generation of $GF(2^8)$ from $GF(2)$ in steps of degree.

EXAMPLE 3-10: Let $p = 2$ and $n = 4$, and suppose that $f(x) = x^2 + x + g$ where g is a primitive element of $GF(2^4)$. Then f is a primitive polynomial (see Example 4.2 below) which generates $GF(2^8)$, and if w is a root of f, then $w^2 + w + g = 0$, i.e., $w^2 = g \cdot 1_4 + 1_8 \cdot w$. By Proposition 3-1, the other root of f is $w^{2^4} = w^{16}$. In order to apply the preceding proposition to write w^{16} in a form with coefficients in $GF(2^4)$, it is necessary to observe that in the context of Proposition 3-9, $j = 0$, $k = 1$, and $s = 0$ and $t = 1$ (since $w = 0 \cdot 1 + 1 \cdot w$). Thus, by (3.2), recalling that 1_4 is the unit element of $GF(2^4)$ and that 1_8 is the unit element of $GF(2^8)$,

$$w^{16} = [(2 - 1) \cdot 1 \cdot \gamma^0 + 0] \cdot 1 + (2 - 1) \cdot 1 \cdot w = 1_8 + 1_4 \cdot w.$$

The conjugate $(w^2)^{2^4} = w^{32}$ of $w^2 = g \cdot 1_8 + 1_4 \cdot w$ (therefore $s = g$ and $t = 1$) with respect to $GF(2^4)$ is

$$w^{32} = [(2 - 1) \cdot 1 \cdot g^0 + g] \cdot 1 + (2 - 1) \cdot 1 \cdot w = (1 + g) \cdot 1 + w = g^2 \cdot 1_8 + 1_4 \cdot w$$

(that $g^{12} = 1_4 + g$ in GF(2^4) can be seen in Table 4-2 in the next section.

Suppose that f(x) as a primitive polynomial of degree 2 over GF(p^{2n}) which generates GF(p^{4n}), and suppose that it is desired to determine a primitive polynomial of degree 4 which generates GF(p^{4n}) over GF(p^n). The following proposition tells how to calculate such a primitive polynomial from f(x). Before stating this proposition, though, the concept of a conjugate polynomial is needed.

Let $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$ and $g(x) = b_k x^k + \cdots + b_1 x + b_0$ be two arbitrary polynomials over GF(p^{2n}). Then f(x) and g(x) are called ***conjugate polynomials*** if a_i and b_i are conjugate elements of GF(p^{2n}) with respect to GF(p^n) for every i = 0, 1, . . ., k. By Proposition 3-1, $b_i = a_i^{p^n}$ for every i.

PROPOSITION 3-11: Let $f(x) = x^2 + \alpha^j x + \alpha^k$ and $g(x) = x^2 + \alpha^{j \cdot p^n} x + \alpha^{k \cdot p^n}$ be conjugate primitive polynomials over GF(p^{2n}). Then the polynomial $r = f \cdot g$, given by

$$r(x) = x^4 + \left(\alpha^j + \alpha^{j \cdot p^n}\right) x^3 + \left(\alpha^{(p^n+1)j} + \alpha^k + \alpha^{k \cdot p^n}\right) x^2 + \left(\alpha^{j+k \cdot p^n} + \alpha^{k+j \cdot p^n}\right) x$$
$$+ \alpha^{k(p^n+1)}.$$

is a primitive polynomial with coefficients in GF(p^n) which generates GF(p^{4n}).

Proof: If γ denotes one root of r(x), the other three roots of r are in the same cyclotomic coset with respect to GF(p^n) as γ, and are given by γ^{p^n}, $\gamma^{p^{2n}}$, and $\gamma^{p^{3n}}$ by Proposition 3-1. Since these four elements satisfy f(x) and g(x), and since f(x) and g(x) are primitive γ, γ^{p^n}, $\gamma^{p^{2n}}$, and $\gamma^{p^{3n}}$ are primitive elements of GF(p^{4n}). Hence r(x) is a primitive polynomial. It only remains to show that the coefficients of r(x) are in GF(p^n).

For convenience, r(x) will be written in the following way:

$$r(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0.$$

It must be shown that a_0, a_1, a_2, and a_3 are all in GF(p^n). This can be done by showing that $(a_i)^{p^n-1} = 1$ for i = 0, 1, 2, 3. First, a_0.

$$(a_0)^{p^n-1} = \left(\alpha^{k(p^n+1)}\right)^{p^n-1} = \alpha^{k(p^{2n}-1)} = \left(\alpha^{p^{2n}-1}\right)^k = 1^k = 1$$

since α is in GF(p^{2n}) (recall that for every element t in GF(p^{2n}), $t^{p^{2n}-1} = 1$). Thus $a_0^{p^n-1} = 1$, and so a_0 is in GF(p^n). Next it is shown that $a_1 = \alpha^{j+k \cdot p^n} + \alpha^{k+j \cdot p^n}$ is in GF(p^n). Before this is done, however, the reader is reminded that for any two elements a and b of GF(p^n), $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ [2, Theorem 6.14] and so

$$\begin{aligned}
a_1{}^{p^n} &= \left(\alpha^{j+k\cdot p^n} + \alpha^{k+j\cdot p^n}\right)^{p^n} = \left(\alpha^{j+k\cdot p^n}\right)^{p^n} + \left(\alpha^{k+j\cdot p^n}\right)^{p^n} \\
&= \left(\alpha^{j} \cdot \alpha^{k\cdot p^n}\right)^{p^n} + \left(\alpha^{k} \cdot \alpha^{j\cdot p^n}\right)^{p^n} = \alpha^{j\cdot p^n} \cdot \alpha^{k\cdot p^{2n}} + \alpha^{k\cdot p^n} \cdot \alpha^{j\cdot p^{2n}} \\
&= \alpha^{j\cdot p^n} \cdot (\alpha^{p^{2n}})^{k} + \alpha^{k\cdot p^n} \cdot (\alpha^{p^{2n}})^{j} = \alpha^{j\cdot p^n} \cdot \alpha^{k} + \alpha^{k\cdot p^n} \cdot \alpha^{j} \\
&= \alpha^{j\cdot p^n+k} + \alpha^{k\cdot p^n+j} = a_1.
\end{aligned}$$

Note that $\alpha^{p^{2n}} = \alpha$ since α is in GF(p^{2n}), i.e., for all nonzero elements of GF(p^{2n}), $\alpha^{p^{2n}} = \alpha$ is equivalent to $\alpha^{p^{2n}-1} = 1$. Similarly, since it has now been shown that $a_1{}^{p^n} = a_1$, it can be concluded that a_1 is in GF(p^n). Next a_2 must be considered.

$$\begin{aligned}
a_2{}^{p^n} &= \left(\alpha^{(p^n+1)j} + \alpha^{k} + \alpha^{k\cdot p^n}\right)^{p^n} = \alpha^{(p^n+1)j\cdot p^n} + \alpha^{k\cdot p^n} + \alpha^{k\cdot p^n\cdot p^n} \\
&= \alpha^{j\cdot p^{2n}} \cdot \alpha^{j\cdot p^n} + \alpha^{k\cdot p^n} + \alpha^{k\cdot p^{2n}} = \left(\alpha^{p^{2n}}\right)^{j} \cdot \alpha^{j\cdot p^n} + \alpha^{k\cdot p^n} + \\
&\qquad \left(\alpha^{p^{2n}}\right)^{k} = \alpha^{j} \cdot \alpha^{j\cdot p^n} + \alpha^{k\cdot p^n} + \alpha^{k} = \alpha^{j\cdot(p^n+1)} + \alpha^{k\cdot p^n} + \alpha^{k} = a_2,
\end{aligned}$$

and so a_2 is in GF(p^n). Next a_3.

$$a_3{}^{p^n} = (\alpha^{j} + \alpha^{j\cdot p^n})^{p^n} = \alpha^{j\cdot p^n} + \alpha^{j\cdot p^n\cdot p^n} = \alpha^{j\cdot p^n} + (\alpha^{p^{2n}})^{j} = \alpha^{j\cdot p^n} + \alpha^{j} = a_3.$$

and so a_3 is in GF(p^n). Thus all the coefficients of r(x) are in GF(p^n) and so r(x) is a primitive polynomial over GF(p^n).

Thus, it is not difficult to design a GF(p^{4n}) Galois multiplier over GF(p^n) if the design of a GF(p^{4n}) multiplier is known over GF(p^{2n}).

SECTION 4
EXAMPLES

4.1 INTRODUCTION

In this section, two examples are given illustrating the concept of subfield multiplication which was discussed in the introduction to this report. Much of the procedure needed to do subfield multiplication is based on the results of the preceding section.

The first example shows the process of constructing GF(2^8) in steps of degree 2, i.e., via GF(2^1) → GF(2^2), GF(2^2) → GF(2^4), and GF(2^4) → GF(2^8). This example is the same one used in reference [6], but it is given in much more detail here. The second example deals with the construction of GF(3^4) from GF(3^2). In both examples it will be shown how to multiply two elements in the larger field by carrying out the actual multiplication in their subfields.

4.2 CONSTRUCTION OF A GF(2^8) MULTIPLIER USING SUBFIELD MULTIPLIERS

To begin the construction of a GF(2^8) Galois linear module using a GF(2^4) multiplier, one starts with a GF(2^2) module using GF(2^1) multipliers, i.e., AND gates. To construct such a module, a primitive polynomial of degree 2 is chosen over GF(2^1). There is exactly one such polynomial, $p(x) = x^2 + x + 1$ [2, page 476]. Let t be a root of p. Then $0 = p(t) = t^2 + t + 1$, and so $t^2 = 1 + t$. Using this equation, the code for the field GF(2^2) = $\{0_2, 1_2, t, t^2\}$ can be easily computed; see Table 4-1. (For example, t has the code 01 since $t = 0 \cdot 1_2 + 1 \cdot t$. In the remainder of this report, the 0 and 1 element of GF(2^m) will be labelled 0_m and 1_m for every m greater than 1.)

TABLE 4-1. A CODE FOR GF(2^2) OVER GF(2^1)

0_2	0	0
1_2	1	0
t	0	1
t^2	1	1

Now the Galois multiplier for GF(2^2) is constructed. If $\{1_2, t\}$ is the ordered basis used, the basis product matrix (see the Appendix) is given by

$$M^{2,1} = \begin{pmatrix} 1_2 \cdot 1_2 & 1_2 \cdot t \\ t \cdot 1_2 & t \cdot t \end{pmatrix} = \begin{pmatrix} 1_2 & t \\ t & t^2 \end{pmatrix} = \begin{pmatrix} 10 & 01 \\ 01 & 11 \end{pmatrix}.$$

Thus, the two component matrices are

$$M_1^{2,1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad M_2^{2,1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Thus, the GF(2^2) multiplier over GF(2^1) can be drawn in Figure 4-1.

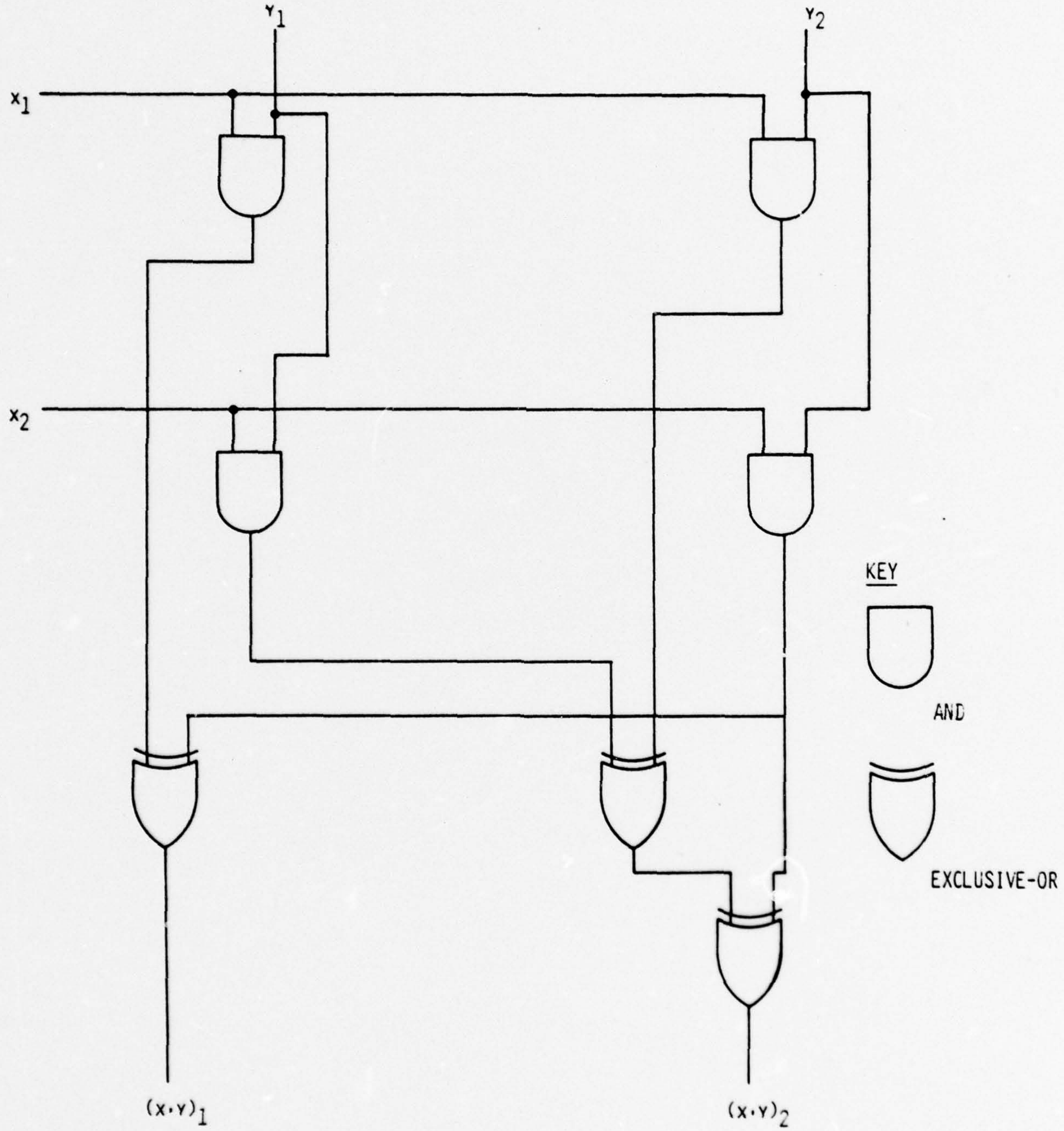

FIGURE 4-1. A GF(2^2) MULTIPLIER OVER GF(2^1)

The next step is to construct a $GF(2^4)$ multiplier out of $GF(2^2)$ multipliers. It can be seen in Table 3-2 that there are 6 irreducible polynomials of degree 2 over $GF(2^2)$ of which 4 are primitive. This fact also follows from Corollary 3-4 since $T = \frac{1}{4}(2^4 - 2^2) = \frac{12}{4} = 3$ is the number of 4–element cosets over $GF(2^2)$, and hence there are $\frac{n}{m} \cdot T = \frac{4}{2} \cdot 3 = 6$ irreducible polynomials of degree $\frac{n}{m} = \frac{4}{2} = 2$ over $GF(2^2)$. Again from Table 3-2, there are two cyclotomic cosets (numbers 3 and 4) which have a factor (3) in common with the order $2^4 - 1 = 15$ of the cyclic group $GF(2^4) - \{0\}$. The primitive polynominal that is used in this discussion is $x^2 + tx + t$. If g denotes a root of $x^2 + tx + t$, then $g^2 = t + tg$, and if $\{1_4, g\}$ is the ordered basis chosen, then the following code (Table 4-2) is obtained for $GF(2^4)$.

TABLE 4-2. A CODE FOR $GF(2^4)$ OVER $GF(2^2)$ AND $GF(2^1)$

$GF(2^4)$	$GF(2^2)$		$GF(2^1)$
0_4	0_2	0_2	0000
1_4	1_2	0_2	1000
g	0_2	1_2	0010
g^2	t	t	0101
g^3	t^2	1_2	1110
g^4	t	1_2	0110
g^5	t	0_2	0100
g^6	0_2	t	0001
g^7	t^2	t^2	1111
g^8	1_2	t	1001
g^9	t^2	t	1101
g^{10}	t^2	0_2	1100
g^{11}	0_2	t^2	0011
g^{12}	1_2	1_2	1010
g^{13}	t	t^2	0111
g^{14}	1_2	t^2	1011

The primitive polynomial $x^2 + tx + t$ used to generate $GF(2^4)$ from $GF(2^2)$ has conjugate polynomial $x^2 + t^2x + t^2$ (see the preceding section for the definition of conjugate polynomial). Thus, by Proposition 3-11, the product of these two polynomials is the primitive polynomial of degree 4 which generates $GF(2^4)$ from $GF(2^1)$. Using Table 4-1 to carry out the calculations in $GF(2^2)$, it is possible to see that $x^4 + x^3 + 1$ is this primitive polynomial over $GF(2^1)$. In fact

$$(x^2 + tx + t)(x^2 + t^2x + t^2) = x^4 + (t + t^2)x^3 + (t^2 + t + 1)x^2 + (t^3 + t^2)x + t^3 = x^4 + x^3 + 1.$$

The next step is to see how $GF(2^4)$ multiplication can be done with $GF(2^2)$ multipliers. Again, the ordered basis which is used here is in $\{1_4, g\}$, and so the multiplication matrix is

$$M^{4,2} = \begin{pmatrix} 1_4 & g \\ g & g^2 \end{pmatrix} = \begin{pmatrix} 1_2\ 0_2 & 0_2 1_2 \\ 0_2\ 1_2 & t\ t \end{pmatrix}$$

Thus, the two component matrices of $GF(2^4)$ over $GF(2^2)$ in this case are

$$M_1{}^{4,2} = \begin{pmatrix} 1_2 & 0_2 \\ 0_2 & t \end{pmatrix} \quad \text{and } M_2{}^{4,2} = \begin{pmatrix} 0_2 & 1_2 \\ 1_2 & t \end{pmatrix}$$

These two matrices tell exactly how to connect the four $GF(2^2)$ multipliers in order to obtain a $GF(2^4)$ multiplier: for example, to obtain the first 2-bit output of the $GF(2^4)$ product, if $M_k{}^{4,2} = (m_{ij})_k{}^{4,2}$, then $(m_{11})_1{}^4$ and $(m_{22})_1{}^{4,2}$ are needed, the latter multiplied by t; similarly, the second 2-bit output is obtained by adding $(m_{12})_2{}^{4,2}$ and $(m_{21})_2{}^{4,2}$ to $(m_{22})_2{}^{4,2}$ times t. To construct a t-multiplier one uses the Beethoven method of Ellison [4]. In particular, the two bits in the t-multiplier are calculated by $(M_t)_1 = t \cdot M_1{}^{2,1} \cdot x^t$ and $(M_t)_2 = t \cdot M_2{}^{2,1} \cdot x^t$ where x^t is the transpose of $x = (x_1 x_2)$ (if x is the row vector $(x_1 x_2)$, then x^t is the column vector $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$); since $t = 01$,

$$(M_t)_1 = (01)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (01)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_2 \qquad \text{and}$$

$$(M_t)_2 = (01)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (11)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \oplus x_2 .$$

Thus, a t-multiplier can be drawn in Figure 4-2.

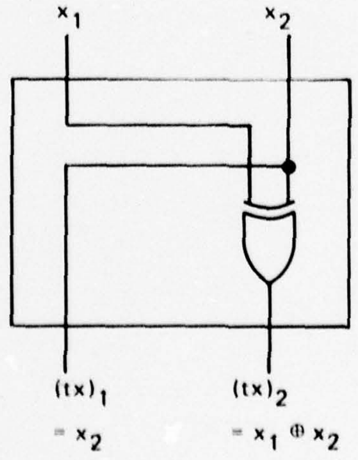

FIGURE 4-2. A CONSTANT t-MULTIPLIER IN $GF(2^2)$

Now a GF(2^4) multiplier over GF(2^2) can be seen in Figure 4-3. Here x and y in GF(2^4) are encoded by x_1x_2 and y_1y_2, each x_i and y_i in GF(2^2).

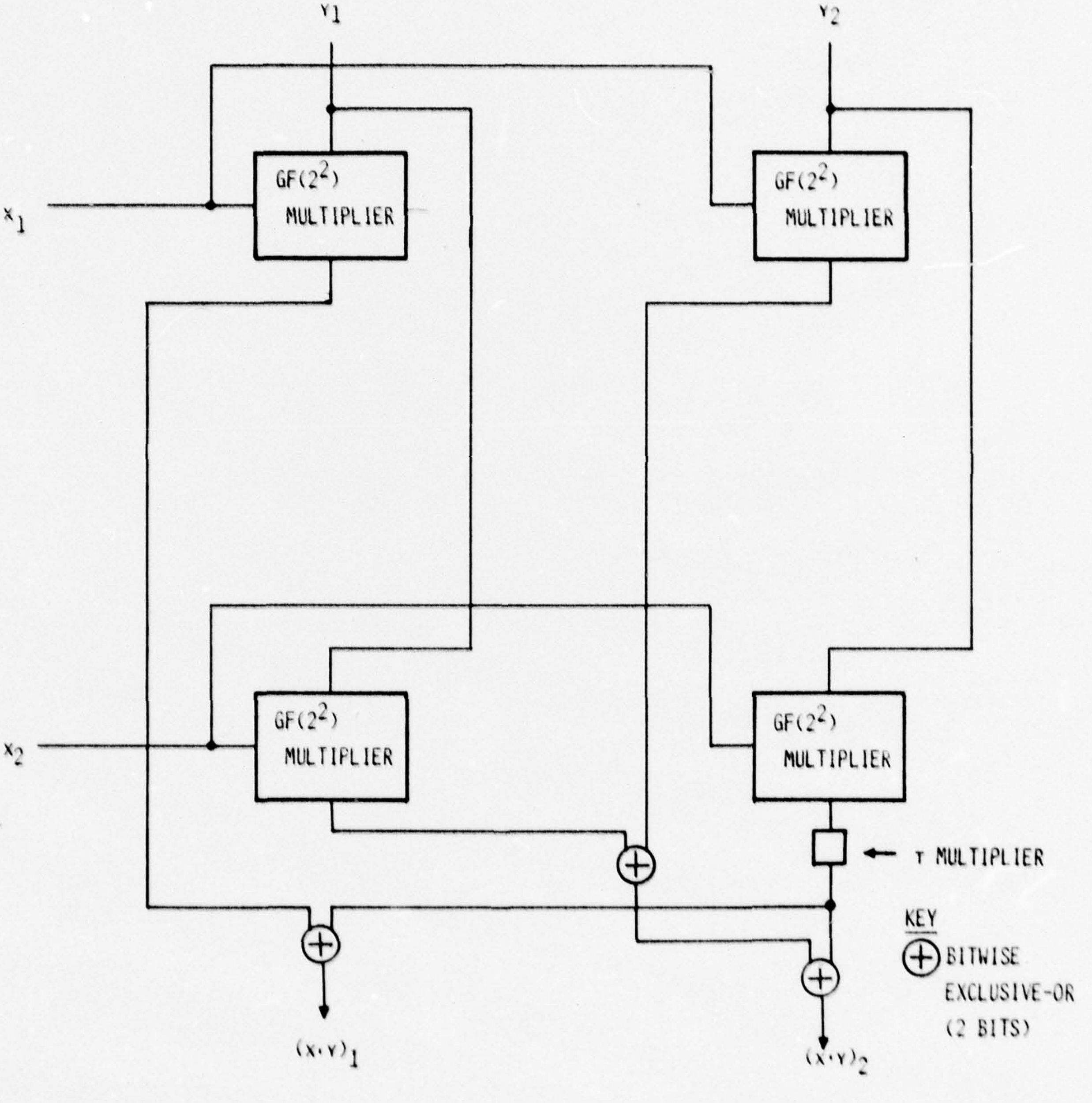

FIGURE 4-3. A GF(2^4) MULTIPLIER OVER GF(2^2)

The next step in order to build a $GF(2^8)$ multiplier over $GF(2^4)$ is to generate a code for $GF(2^8)$ over $GF(2^4)$. In Example 3-8 it was shown that there are 30 irreducible polynomials of degree 8 over $GF(2)$ of which 16 are primitive (see Table 3-3). By Corollary 3-4 there are $\frac{8}{2} \cdot 16 = 64$ primitive polynomials of degree 2 over $GF(2^4)$. The one chosen here is $p(x) = x^2 + x + g$. One root of this equation in $GF(2^8)$ is called w, and therefore the other one is $w^{2^4} = w^{16}$, by Proposition 3-1. Hence w satisfies the equation $w^2 = w + g$ and from this equation the entire field $GF(2^8)$ minus 0 can be written as a power of w. The ordered basis used for generating $GF(2^8)$ over $GF(2^4)$ is $\{1_8, w\}$ and so the basis matrix for $GF(2^8)$ over $GF(2^4)$ is

$$M^{8,4} = \begin{pmatrix} 1_8 & w \\ w & w^2 \end{pmatrix} = \begin{pmatrix} 1_4\,0_4 & 0_4\,1_4 \\ 0_4\,1_4 & g\;\;1_4 \end{pmatrix}$$

Thus,

$$M_1^{8,4} = \begin{pmatrix} 1_4 & 0_4 \\ 0_4 & g \end{pmatrix} \quad \text{and} \quad M_2^{8,4} = \begin{pmatrix} 0_4 & 1_4 \\ 1_4 & 1_4 \end{pmatrix}$$

Once again a constant multiplier is needed in a subfield multiplier, in this case a constant g-multiplier. As in the case of the constant t-multiplier described earlier in this section, the g-multiplier is constructed by the Beethoven method. Before describing the construction of the constant g-multiplier, Figure 4-4 shows the $GF(2^8)$ multiplier over $GF(2^4)$. Note the similarities of this multiplier to the $GF(2^2)$ multiplier over $GF(2^1)$ in Figure 4-1, and the $GF(2^4)$ multiplier over $GF(2^2)$ in Figure 4-3.

Now, for the constant g-multiplier. From Table 4-2, the ordered basis of $GF(2^4)$ over $GF(2^1)$ consisting of unit vectors is given by $\{1_4, g^5, g, g^6\} = \{1000, 0100, 0010, 0001\}$. Again using the basis product matrix method and the Beethoven reduction method, the g-multiplication gate can be determined:

$$M^{4,1} = \begin{pmatrix} 1 & g^5 & g & g^6 \\ g^5 & g^{10} & g^6 & g^{11} \\ g & g^6 & g^2 & g^7 \\ g^6 & g^{11} & g^7 & g^{12} \end{pmatrix} = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0001 & 0011 & 1111 & 1010 \\ 0001 & 0011 & 1111 & 1010 \end{pmatrix}$$

$$M_1^{4,1} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0011 \end{pmatrix} \qquad M_2^{4,1} = \begin{pmatrix} 0100 \\ 1100 \\ 0011 \\ 0010 \end{pmatrix} \qquad M_3^{4,1} = \begin{pmatrix} 0010 \\ 0001 \\ 1001 \\ 0111 \end{pmatrix} \qquad M_4^{4,1} = \begin{pmatrix} 0001 \\ 0011 \\ 0111 \\ 1110 \end{pmatrix}$$

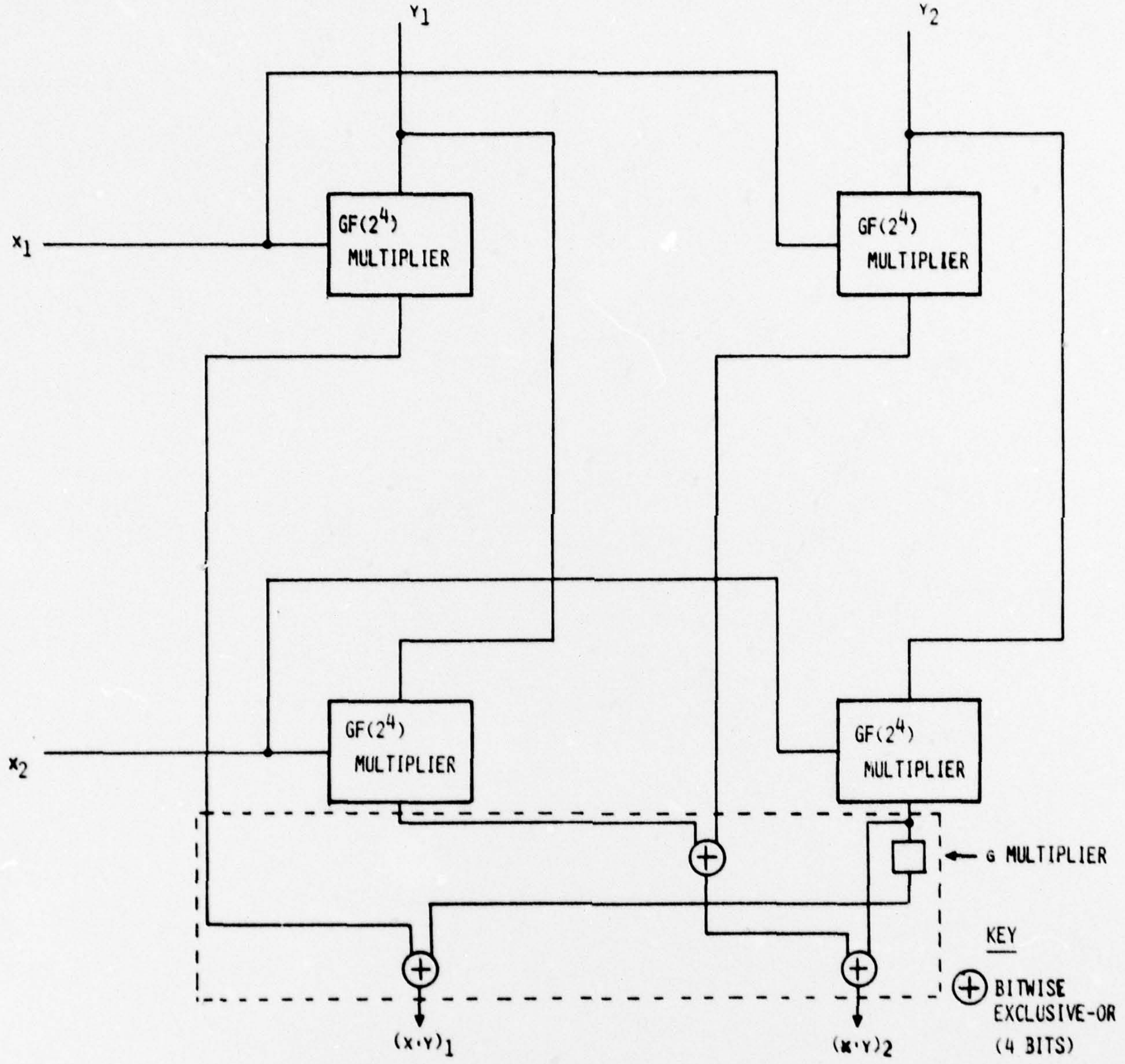

FIGURE 4-4. A GF(2^8) MULTIPLIER OVER GF(2^4)

Thus,

$$(M_g)_1 = (0010) \begin{pmatrix}1000\\0100\\0001\\0011\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = (0001)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = x_4$$

$$(M_g)_2 = (0010) \begin{pmatrix}0100\\1100\\0011\\0010\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = (0011)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = x_3 \oplus x_4$$

$$(M_g)_3 = (0010) \begin{pmatrix}0010\\0001\\1001\\0111\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = (1001)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = x_1 \oplus x_4$$

$$(M_g)_4 = (0010) \begin{pmatrix}0001\\0011\\0111\\1110\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = (0111)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix} = x_2 \oplus x_3 \oplus x_4$$

It can now be concluded that the g-multiplication gate is as shown in Figure 4-5.

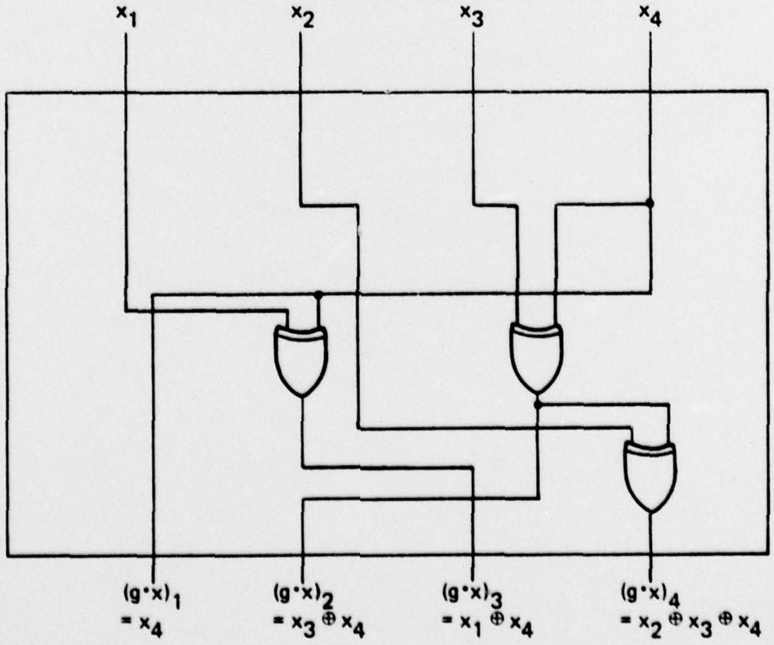
x_1
x_2
x_3
x_4
$(g \cdot x)_1 = x_4$
$(g \cdot x)_2 = x_3 \oplus x_4$
$(g \cdot x)_3 = x_1 \oplus x_4$
$(g \cdot x)_4 = x_2 \oplus x_3 \oplus x_4$

FIGURE 4-5. A CONSTANT g-MULTIPLIER IN GF(2^4)

It turns out that subfield multiplication can be done bit-serially. By computing in this manner, it takes only one GF(2^4) multiplier to do GF(2^8) multiplication as Figure 4-6 shows. It is believed that the advantages of bit-serial implementation are most strongly felt for very large n when the underlying multiplier becomes prohibitively large. Here, multilevel logic may have a strong impact also. However, with or without multilevel logic, subfield multipliers offer much potential for complexity reduction.

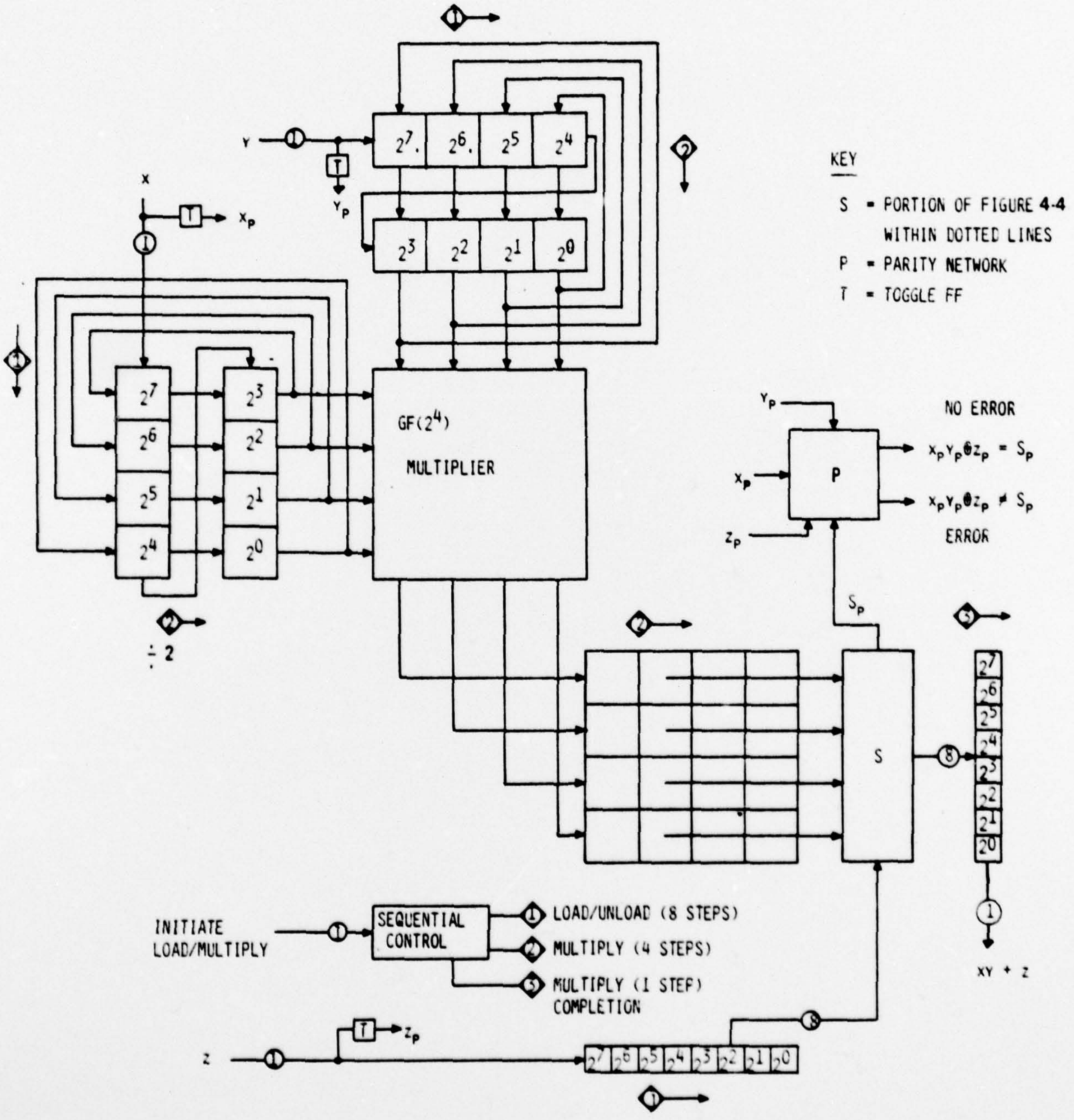

FIGURE 4-6. A 13-STEP GF(2^8) GALOIS LINEAR MODULE (BIT SERIAL INTERFACE)

A natural question at this point is to ask whether it is possible to use the technique stated above to build $GF(2^8)$ multipliers out of $GF(2^2)$ multipliers. The answer is in the affirmative, and the process is described below.

To begin with, recall from Proposition 3-11 that a primitive polynomial of degree 4 over $GF(2^2)$ can be obtained from a primitive polynomial of degree 2 over $GF(2^4)$ by multiplying the latter polynomial by its conjugate polynomial. (See the definition of conjugate polynomial in the paragraph preceding Proposition 3-11.) Since $x^2 + x + g$ is the original polynomial, its conjugate is $x^2 + x + (g)^{2^2} = x^2 + x + g^4$ (by Proposition 3-1, $g^{2^2} = g^4$ is the conjugate of g in $GF(2^4)$ with respect to $GF(2^2)$). Therefore, the primitive polynomial generating $GF(2^8)$ from $GF(2^2)$ in this case is

$$(x^2 + x + g)\,(x^2 + x + g^4) = x^4 + 0 \cdot x^3 + (g + g^4 + 1) \cdot x^2 + (g + g^4)\,x + g^5 = x^4 + t^2\,x^2 + t\,x + t$$

(See Table 4-2 for the computations.) To determine the basis of unit vectors of $GF(2^8)$ over $GF(2^2)$, $\{1_2 0_2 0_2 0_2, 0_2 1_2 0_2 0_2, 0_2 0_2 1_2 0_2, 0_2 0_2 0_2 1_2\}$, one simply notices that this set is the same as $\{1_4 0_4, g0_4, 0_4 1_4, 0_4 g\}$(see Table 4-2). Since $1_8 = 1_4 0_4$ and $w = 0_4 1_4$, it is necessary only to determine j and k so that $w^j = g0_4$ and $w^k = 0_4 g$ (recall that $g0_4$ is shorthand for $g \cdot 1_8 + 0_4 \cdot w = g$). Observe that $w^j = (g0_4)$ is in $GF(2^4)$ and so $(w^j)^{15} = 1 = w^{0(\mathrm{mod}\ 255)}$. Hence, $15j = 255$ and so $j = 17$. Finally, since $w^k = 0_4 \cdot 1 + g \cdot w = w^{17} \cdot w = w^{18}$. Thus, the ordered basis of unit vectors for $GF(2^8)$ over $GF(2^2)$ is $\{1g, w^{17}, w, w^{18}\}$, and as the basis product matrix is

$$M^{8,2} = \begin{pmatrix} 1_8 & w^{17} & w & w^{18} \\ w^{17} & w^{34} & w^{18} & w^{35} \\ w & w^{18} & w^2 & w^{19} \\ w^{18} & w^{35} & w^{19} & w^{36} \end{pmatrix}$$

Using the facts that t is embedded in $GF(2^8)$ as w^{85} ($(w^{85})^3 = w^{255} = 1$) and t^2 is embedded as w^{170}, and that $x^4 + t^2\,x^2 + t\,x + t$ is the primitive polynomial used to generate $GF(2^8)$ from $GF(2^2)$, it is possible to see that

$$M^{8,2} = \begin{pmatrix} 1_2 0_2 0_2 0_2 & 0_2 1_2 0_2 0_2 & 0_2 0_2 1_2 0_2 & 0_2 0_2 0_2 1_2 \\ 0_2 1_2 0_2 0_2 & t\ \ t\ \ 0_2 0_2 & 0_2 0_2 0_2 1_2 & 0_2 0_2 t\ \ t \\ 0_2 0_2 1_2 0_2 & 0_2 0_2 0_2 1_2 & 0_2 1_2 1_2 0_2 & t\ \ t\ \ 0_2 1_2 \\ 0_2 0_2 0_2 1_2 & 0_2 0_2 t\ \ t & t\ \ t\ \ 0_2 1_2 & t^2\, 1_2 t\ \ t \end{pmatrix}$$

Therefore, the four component matrices are

$$M_1{}^{8,2} = \begin{pmatrix} 1_2 & 0_2 & 0_2 & 0_2 \\ 0_2 & t & 0_2 & 0_2 \\ 0_2 & 0_2 & 0_2 & t \\ 0_2 & 0_2 & t & t^2 \end{pmatrix} \qquad M_2{}^{8,2} = \begin{pmatrix} 0_2 & 1_2 & 0_2 & 0_2 \\ 1_2 & t & 0_2 & 0_2 \\ 0_2 & 0_2 & 1_2 & t \\ 0_2 & 0_2 & t & 1_2 \end{pmatrix}$$

$$M_3{}^{8,2} = \begin{pmatrix} 0_2 & 0_2 & 1_2 & 0_2 \\ 0_2 & 0_2 & 0_2 & t \\ 1_2 & 0_2 & 1_2 & 0_2 \\ 0_2 & t & 0_2 & t \end{pmatrix} \qquad M_4{}^{8,2} = \begin{pmatrix} 0_2 & 0_2 & 0_2 & 1_2 \\ 0_2 & 0_2 & 1_2 & t \\ 0_2 & 1_2 & 0_2 & 1_2 \\ 1_2 & t & 1_2 & t \end{pmatrix}$$

Now, using the same procedure for constructing a t-multiplier it is possible to construct a constant t^2-multiplier. Finally, the entire GF(2^8) multiplier built out of $(\frac{8}{2})^2 = 16$ GF(2^2) multipliers can be designed. It is also possible to design the GF(2^8) multiplier out of a single GF(2^2) multiplier by sequentially inserting the inputs as it is done for the GF(2^8) multiplier over GF(2^4) (see Figure 4-6).

4.3 CONSTRUCTION OF A GF(3^4) MULTIPLIER USING SUBFIELD MULTIPLIERS

In this example a GF(3^4) Galois multiplier is constructed out of GF(3^2) multipliers. To begin with, GF(3) = {0,1,2 } and the operations of addition and multiplication in GF(3) are given by addition and multiplication modulo 3, a generalization of GF(2) arithmetic.

In order to construct GF(3^2) from GF(3), the primitive polynomial $p(x) = x^2 + 2x + 2$ is used. If a root of p is labeled a, then $a^2 = a + 1$ (since $2 = -1$ modulo 3), and the ternary code for GF(3^2) with ordered basis {1,a } is shown in Table 4-3.

TABLE 4-3. TERNARY CODE FOR GF(3^2)

	1	a		1	a
0	0	0	a^4	2	0
1	1	0	a^5	0	2
a	0	1	a^6	2	2
a^2	1	1	a^7	2	1
a^3	1	2			

The multiply matrix for GF(3^2) is

$$M = \begin{pmatrix} 1 & a \\ a & a^2 \end{pmatrix} = \begin{pmatrix} 10 & 01 \\ 01 & 11 \end{pmatrix}$$

and so

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Thus, a GF(3^2) multiplier for the ternary code is illustrated in Figure 4-7.

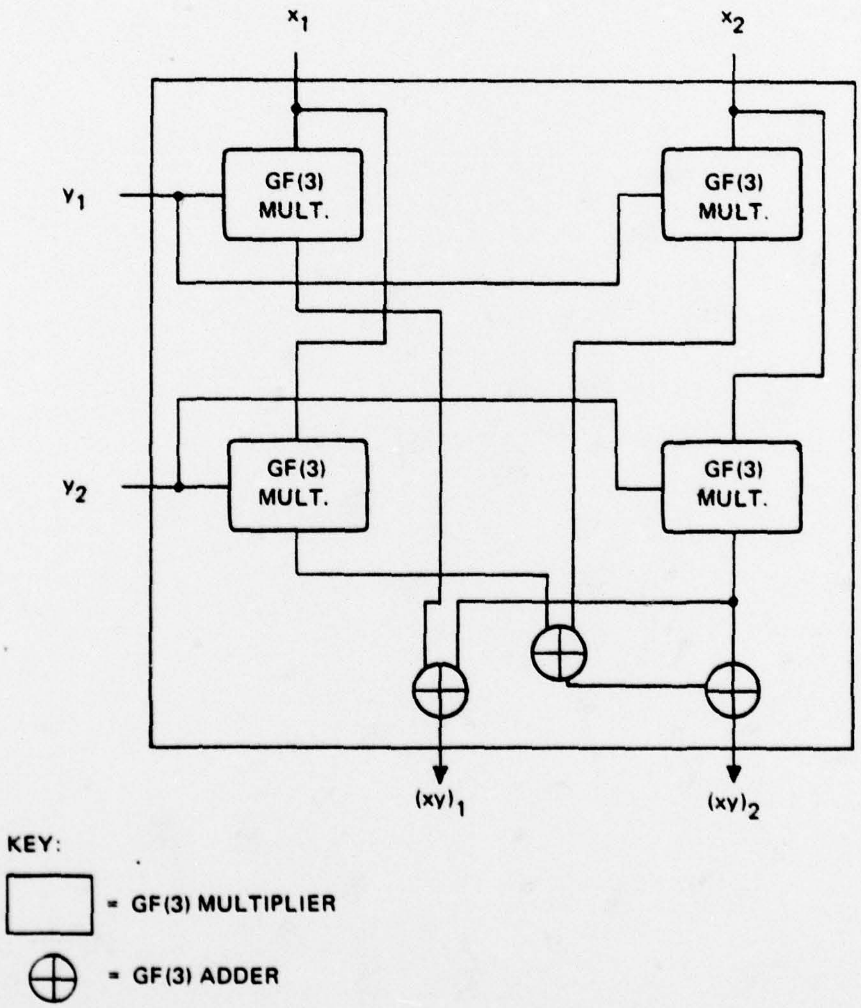

FIGURE 4-7. A GF(3^2) MULTIPLIER OVER GF(3)

By Proposition 3-3 there are

$$T = \frac{1}{4}\ \{ 3^4 - 3^2 \} = \frac{1}{4}\ \{81 - 9\} = \frac{1}{4} \cdot 72 = 18$$

cyclotomic cosets of length 4 in GF(3^4). Hence, by Corollary 3-4 there are mT = 2·18 = 36 2-element cyclotomic cosets in GF(3^4) with respect to GF(3^2). In Table 4-4 below it can be seen that only 8 of the cosets in GF(3^4) over GF(3) have no factor in common with the order, $3^4 - 1 = 80$ of the cyclic group GF(3^4) - {0} of GF(3^4).

TABLE 4-4. TERNARY COSETS IN GF(3^4) WITH LOWEST EXPONENT IN EACH CLASS NAMED
(1 is $\{b^1, b^3, b^9, b^{27}\}$, 2 is $\{b^2, b^6, b^{18}, b^{54}\}$, ETC.)

	COSET	PRIMITIVE MINIMUM POLYNOMIAL		COSET	PRIMITIVE MINIMUM POLYNOMIAL
1.	1	YES	13.	20	(2 ELEMENT COSET)
2.	2	NO	14.	22	NO
3.	4	NO	15.	23	YES
4.	5	NO	16.	25	NO
5.	7	YES	17.	26	NO
6.	8	NO	18.	40	(1 ELEMENT COSET)
7.	10	(2 ELEMENT COSET)	19.	41	YES
8.	11	YES	20.	44	NO
9.	13	YES	21.	50	(2 ELEMENT COSET)
10.	14	NO	22.	53	YES
11.	16	NO	23.	80	(1 ELEMENT COSET)
12.	17	YES			

Hence, these 8·4 = 32 elements are primitive, and are, of course, primitive with respect to GF(3^2). Thus, there are 16 2-element cyclotomic cosets of primitive elements in GF(3^4) with respect to GF(3^2), and so there are 16 primitive polynomials of degree 2 over GF(3^2) with which to generate GF(3^4). The one used here is $g(x) = x^2 + x + a$. If b is a root of g(x) in GF(3^4), then $0 = b^2 + b + a$ and so $b^2 = - a - b = 2a + 2b$. A close look at Table 4-3 shows that GF(3) viewed as a subfield of GF(3^2) consists of the elements 0,1, and a^4 ($0 \rightarrow 0$, $1 \rightarrow 1$, and $2 \rightarrow a^4$) and so $b^2 = 2a \cdot 1 + 2b = a^4\ a \cdot 1 + a^4 \cdot b = a^5 \cdot 1 + a^4 \cdot b$, with coefficients in GF(3^2). Thus, the basis product matrix for GF(3^4), with respect to the basis {1,b}, is

$$M = \begin{pmatrix} 1 & b \\ b & b^2 \end{pmatrix} = \begin{pmatrix} 10 & 01 \\ 01 & a^5a^4 \end{pmatrix} = \begin{pmatrix} 10 & 01 \\ 01 & a^52 \end{pmatrix}$$

and so

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & a^5 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & a^4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$$

From M_1 and M_2 it can be seen that constant multipliers for $a^4(=2)$ and a^5 are needed to build the $GF(3^4)$ multiplier over $GF(3^2)$ by the Beethoven reduction method [4]. For a^4 multiplication by an arbitrary element $z = z_1z_2$ of $GF(3^4)$ with z_1 and z_2 in $GF(3^2)$, is the same as multiplication by 2:

$$a^4; \quad (20)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (20)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = 2z_1$$

$$(20)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (02)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = 2z_2$$

and, for a^5

$$a^5; \quad (02)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (02)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = 2z_2$$

$$(02)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (22)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = 2z_1 + 2z_2$$

Thus, the multipliers for a^4 and a^5 are shown in Figure 4-8 and are very simple compared to the complexity of the total $GF(3^2)$ multiplier, as can be seen in Figure 4-6. Here are two elements $x = x_1x_2$ and $y = y_1y_2$ in $GF(3^4)$, with x_i and y_i in $GF(3^2)$, are multiplied together.

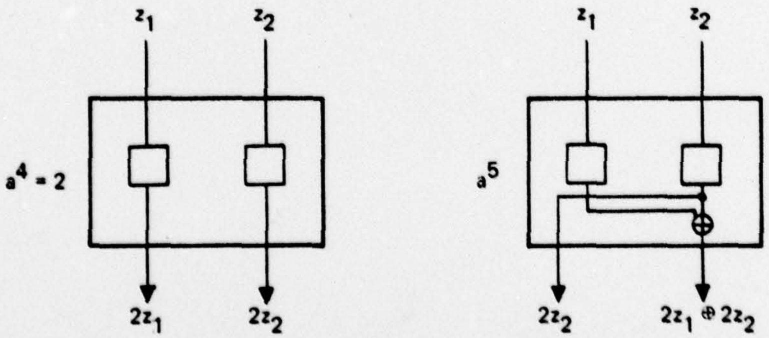

FIGURE 4-8. CONSTANT $a^4 = 2$ AND a^5 MULTIPLIERS

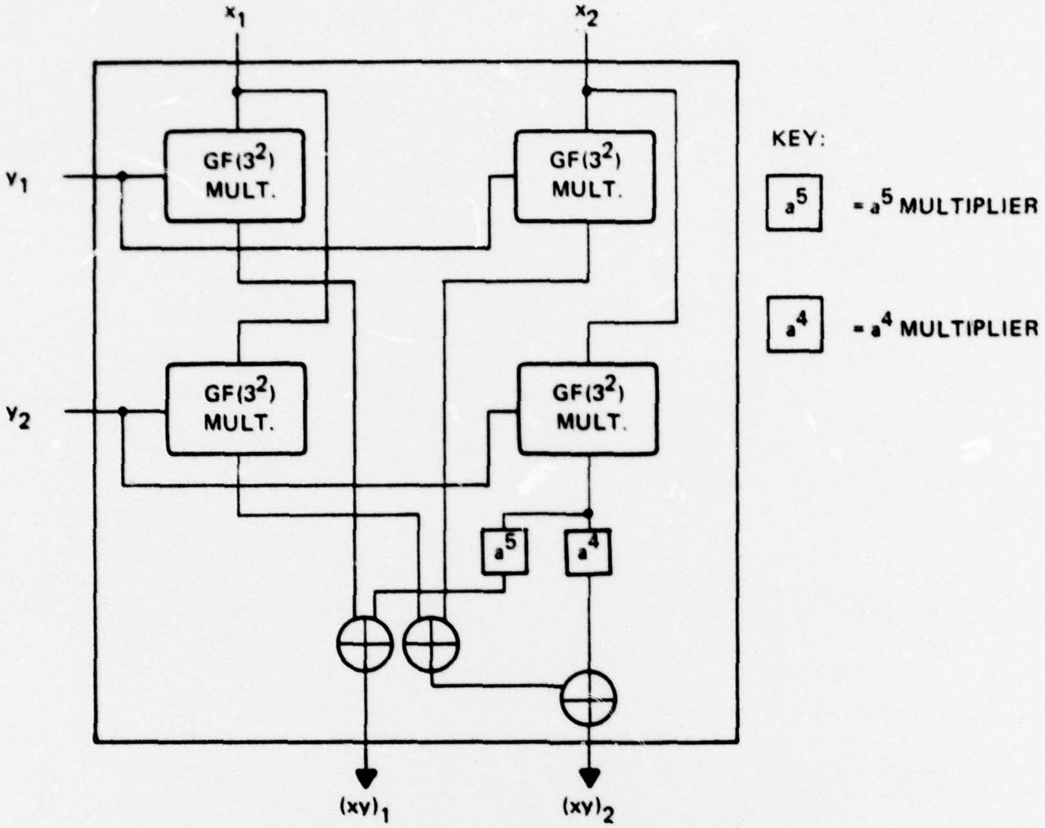

FIGURE 4-9. A GF(3^4) MULTIPLIER OVER GF(3^2)

SECTION 5
SUMMARY

A method of multiplying in arbitrary Galois fields by doing the actual multiplication in a subfield is presented in this report. The process can be carried out either in a parallel fashion or bit-serially. A theoretical discussion in Paragraph 3.3 establishes a basis for this subfield multiplication process. The two examples in Section 4 show the implementation of the process both in binary and ternary fields.

SECTION 6
FUTURE WORK

One of the most important applications of Galois fields is signal processing (see, for example, [5] and [7]). The Galois fields involved in the discussions of Reed, et al, are for the most part of the form GF(p) or GF(p^2) for very large and very special primes p. These primes are such that the cyclic group GF(p) - {0} has order a multiple of a power of two. Therefore it is possible that the subfield multiplication process presented in this report generalizes to a subgroup multiplication process, and that presents GF(2^n) multipliers can be used to perform GF(p) or GF(p^2) arithmetic. If so, the added on-line fault detection implicit in GF(2^n) multipliers can be utilized to do GF(p^n) arithmetic. Therefore, an investigation of the potential of subgroup multiplication is needed in order to determine the feasibility of applying known techniques to do GF(p^n) arithmetic.

Other methods of performing Galois field arithmetic for large p should be investigated also. In particular, hardware implementation of modular Galois arithmetic should be investigated.

Another important application of Galois fields is error coding where a semi-fast Fourier transform algorithm has been developed for use in Galois fields GF(2^n) [8]. The use of present GF(2^n) multipliers are possible here, and it is important to study the potential of the use of the Galois multiplier which has the on-line parity detection. In this case there would be a check (parity bit) on the checker (code).

APPENDIX

BASIS PRODUCT MATRICES

Let B = $\{ b_i \}$ be an ordered basis in GF(p^n) over GF(p^m), which consists of $\frac{n}{m}$ elements and let

$$x = \sum_{i=1}^{n/m} x_i b_i \quad \text{and} \quad y = \sum_{j=1}^{n/m} y_j b_j \text{, p any prime.}$$

Then the product xy is

$$\sum_{i,j} x_i y_j b_i b_j$$

Let $b_{ij} = b_i b_j$ and define $M_k{}^{n,m} = (m_{ij})_k{}^{n,m}$ be defined by

$$b_{ij} = \sum_{k=1}^{n/m} (m_{ij})_k{}^{n,m} b_k$$

Then $xy = (\sum_i x_i b_i)(\sum_j y_j b_j) = \sum_i \sum_j x_i y_j b_{ij} = \sum_i \sum_j x_i y_i \sum_k (m_{ij})_k{}^{n,m} b_k$

$$= \sum_k [\sum_i \sum_j x_i y_j (m_{ij})_k{}^{n,m}] b_k .$$

Therefore, if $xy = \sum_k z_k b_k$, $z_k = \sum_i \sum_j x_i y_j (m_{i\,j})_k{}^{n,m} = y M_k{}^{n,m} x^t$.

The matrix $M_k{}^{n,m}$ is called the *kth component basis product matrix* and $M^{n,m} = (M_k{}^{n,m})$ is called the *basis product matrix* for GF(p^n) over GF(p^m).

EXAMPLE: Let n=4 and m=2. Then $\frac{n}{m} = \frac{4}{2} = 2$. Let B = $\{ 1,g \}$ and pick $x = g^7 = t^2 + t^2 \cdot g$ and $y = g^{11} = t^2 \cdot g$ (see Table 4-2). Then the basis product matrix $M^{4,2}$ is

$$M^{4,2} = \begin{pmatrix} 1_4 \cdot 1_4 & 1_4 \cdot g \\ g \cdot 1 & g \cdot g \end{pmatrix} = \begin{pmatrix} 1_4 & g \\ g & g^2 \end{pmatrix} = \begin{pmatrix} 1_2 0_2 & 0_2 1_2 \\ 0_2 1_2 & t \ t \end{pmatrix}$$

$$M_1{}^{4,2} = \begin{pmatrix} 1_2 & 0_2 \\ 0_2 & t \end{pmatrix} \qquad M_2{}^{4,2} = \begin{pmatrix} 0_2 & 1_2 \\ 1_2 & t \end{pmatrix}$$

If $xy = \sum_{k=1}^{2} z_k w_k = z_1 \cdot 1_2 + z_2 \cdot t$, then

$$z_1 = g^{11} \begin{pmatrix} 1_2 & 0_2 \\ 0_2 & t \end{pmatrix} (g^7)^t = (0_2 t_2) \begin{pmatrix} 1_2 & 0_2 \\ 0_2 & t \end{pmatrix} \begin{pmatrix} t^2 \\ t^2 \end{pmatrix} = (0_2 1_2) \begin{pmatrix} t^2 \\ t^2 \end{pmatrix} = t^2$$

$$z_2 = g^{11} \begin{pmatrix} 0_2 & 1_2 \\ 1_2 & t \end{pmatrix} (g^7)^t = (0_2 t^2) \begin{pmatrix} 0_2 & 1_2 \\ 1_2 & t \end{pmatrix} \begin{pmatrix} t^2 \\ t^2 \end{pmatrix} = (t^2 1_2) \begin{pmatrix} t^2 \\ t^2 \end{pmatrix} = 1_2$$

$xy = t^2 \cdot 1_4 + 1_2 \cdot g = (t^2 1_2) = g^3$ (see Table 4-2.) Since $g^{11} \cdot g^7 = g^{18} = g^3$ (3 = 18 modulo ($2^4 - 1$)),the answer is correct.

BIBLIOGRAPHY

[1] Ellison, J. T., "Universal Function Theory and Galois Logic Studies," Univac DSD, Final Report to Air Force Cambridge Research Laboratories, March 1972.

[2] Peterson, W.W. and Weldon, Jr., E. J., Error Correcting Codes, Second Edition, The MIT Press, 1972.

[3] Birkhoff, G. and MacLane, S., A Summary of Modern Algebra, The Macmillan Company, 1963.

[4] Ellison, J. T., "Beethoven Reductions of Galois Networks," Univac DSD, PX-10144, September 1973.

[5] Reed, I. S., "The Use of Finite Fields and Rings to Compute Convolutions," Lincoln Lab, MIT, June 1975.

[6] Marver, J. M., "Sequential Galois Multipliers," Univac DSD, PX-12344, August 1977.

[7] Reed, I. S., Truong, T. K., Kwoh, Y. S., and Hall, E. L., "Image Processing by Transforms Over a Finite Field," IEEE Transactions on Computers, Vol. C-26, No. 9, September 1977.

[8] Sarwate, D. V., "A Semi-Fast Fourier Transform Algorithm Over GF(2^m), R-735, Coordinated Science Lab, University of Illinois, September 1976.